

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION**

IN RE: BLACKBAUD, INC. CUSTOMER
DATA SECURITY BREACH LITIGATION

Case No. 3:20-mn-02972-JMC

MDL No. 2972

**AMENDED CONSOLIDATED
CLASS ACTION COMPLAINT**

REDACTED VERSION

TABLE OF CONTENTS

	<u>Page</u>
II. NATURE OF THE ACTION	6
III. PARTIES	20
A. Plaintiffs	20
B. Defendant.....	86
IV. JURISDICTION AND VENUE	87
V. STATEMENT OF FACTS	88
A. A Sophisticated Cloud-Service Provider, Blackbaud Knew of the Risk That Cybercriminals Posed to Hosted Data	88
B. Blackbaud’s Responsibility to Safeguard Information	107
C. Blackbaud Failed to Meet Its Obligations to Protect Private Information or Comply with its own Privacy Policies	108
D. Blackbaud Failed to Comply with Industry and Regulatory Standards.....	111
E. Blackbaud’s Failures Resulted in a Data Breach.....	115
F. Data Breaches Put Consumers at Increased Risk of Fraud and Identity Theft.....	134
G. Blackbaud’s Inadequate Response to the Data Breach.....	141
VI. PLAINTIFFS’ AND CLASS MEMBERS’ INJURIES AND DAMAGES	147
A. Plaintiffs’ and Class Members’ Private Information was Compromised in the Data Breach.....	147
B. The Private Information of Minors Was Also Compromised in the Data Breach	152
C. Plaintiffs’ and Class Members’ PHI was Compromised in the Data Breach	155
VII. CLASS ACTION ALLEGATIONS	160
VIII. CAUSES OF ACTION	164
A. CLAIMS ON BEHALF OF THE NATIONWIDE CLASS	170
B. CLAIMS ON BEHALF OF THE STATE SUBCLASSES	185
IX. PRAYER FOR RELIEF	408
X. JURY TRIAL DEMAND	409

AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs, identified in Section III.A. below, individually and on behalf of all others similarly situated (“Plaintiffs”), bring this action against Defendant Blackbaud, Inc. (“Blackbaud”), seeking monetary damages, restitution, and/or injunctive relief regarding Blackbaud’s cybersecurity practices. Plaintiffs also seek an injunction to require Blackbaud to fix its incomplete and misleading notices from 2020 that omit material information about the data breach that is the subject of this lawsuit; fail to disclose other attacks at that time; and state without corroboration and contrary to its advisors that it secured confirmation that stolen customer data was deleted. Plaintiffs make the following allegations upon personal knowledge, information and belief derived from, among other things, investigation of their counsel and facts that are a matter of public record, and upon discovery of Blackbaud’s employees, including its former Chief Information Security Officer.

I. INTRODUCTION

1. This lawsuit exists because cybercriminals unsurprisingly targeted a company in the business of storing personal information, stealing the valuable personal information and demanding payment to supposedly delete the data that they stole. Such a payment, or a “ransom,” is paid by companies who acquiesce to data publication extortion demands when they are trying to prevent the public, victims, and shareholders from learning about a data breach.¹ After data was stolen from its servers, Blackbaud paid a ransom for the cybercriminals’ assurances that stolen data was “deleted.” But the breach became public anyway. Now, Blackbaud is trying to spin its

¹ Brian Krebs, *Why Paying to Delete Stolen Data is Bonkers*, Krebs on Security (Nov. 20, 2020), <https://krebsongsecurity.com/2020/11/why-paying-to-delete-stolen-data-is-bonkers/> [<https://perma.cc/34EL-W393>].

extortion payment as its way of having successfully “stopped” a ransomware attack, despite the fact that cybercriminals had already stolen the very data Blackbaud was entrusted to protect.

2. Worse, Blackbaud’s spin omits or misstates material information about the attack and the supposed confirmation of the deletion, wrongly reassuring its customers, and the public (including Class members), that the stolen data will not be exploited. Action is required so that individuals may protect themselves from further injury.

3. Blackbaud is a successful data security company, having created a niche market in—and profiting handsomely from—data security for some of the most highly-sensitive information that exists: personal information from donors, patients, students, and congregants.

4. The value of this information is recognized by several, different constituencies. First, the value is recognized by Blackbaud, which can attribute its business model to the existence of this information, and the need to keep it safe. Second, the value is recognized by cybercriminals, who know that this type of data can be exploited for ransom payments and to commit identity theft. And third, the value is recognized by the individuals, themselves, whose data was stolen.

5. Blackbaud identifies itself as the “world’s leading cloud software company powering social good,” a job on which it claims to have been “100% focused” “[s]ince day one.”² Blackbaud markets its expertise in safeguarding information to those organizations who normally do not have access to high-level information security (such as art and cultural organizations, companies, faith communities, foundations, healthcare organizations, higher education institutions, individual change agents, K-12 schools, and nonprofit organizations)—not only because statutory schemes require certain levels of data security, but to thwart cybersecurity

² About Blackbaud, <https://www.blackbaud.com/company> (last visited Dec. 19, 2020) [https://perma.cc/PQ95-EE6A].

attacks. These vulnerable “Social Good Entities,” as described below, rely on Blackbaud to deliver the strong security practices it promises, because their donors, students, patients, and congregants count on the security of their data in order to engage with these organizations.

6. Millions of individuals have shared their most valuable data with Social Good Entities based on the ordinary, reasonable understanding that their information would be handled and maintained with appropriate safety standards—the very services that Blackbaud was engaged to and promised to perform.

7. Despite Blackbaud’s representations that it provided robust cybersecurity services, in reality, its security program was woefully inadequate—a fact known, but not corrected by Blackbaud. Blackbaud’s unsound, vulnerable systems containing valuable data were an open invitation for a months-long intrusion and exfiltration by cybercriminals, who were seeking to exploit the valuable nature of the information to extract a ransom from Blackbaud, among other unlawful activities.

8. Rather than disclose the theft and initiate protections for the victims, Blackbaud remained silent for months while secretly attempting to buy off the anonymous criminals who had stolen and then held this valuable data hostage, paying a handsome ransom. Apparently relying only on the concept of “honor among thieves,” Blackbaud claims that the anonymous cybercriminals who breached its systems, stole the valuable and sensitive data, and held it ransom, were trustworthy and could be counted on for the level of responsibility, fidelity, and security for private data that Blackbaud itself failed to show.

9. Privately, its own Chief Information Security Officer (“CISO”) warned that

[REDACTED] .³ [REDACTED]

³ Deposition of Rich Friedberg (“Friedberg Dep.”) at 286:10-18, 288:18-289:3l; PX26.

[REDACTED]⁴ Finally, contrary to its messaging, [REDACTED]

[REDACTED].⁵

10. Despite guidance from the federal government, regulatory bodies, and cybersecurity professionals warning companies *not* to pay ransoms to cybercriminals, Blackbaud negotiated payment, and now asserts that it “discovered and stopped a ransomware attack.”⁶ [REDACTED]

[REDACTED].⁷

[REDACTED].⁸ Further, Blackbaud’s payment has only demonstrated that it was willing to make at least one payment to prevent the data from being disclosed—a powerful message to individuals with access to the very information that facilitates identity theft and health insurance fraud.

11. Additionally, the “honor among thieves” principal only makes sense when the cybercriminal is operating under a name it will later use to gain the trust of other companies it is attacking. However, as the cybercriminal who performed the Blackbaud attack was anonymous, Blackbaud had even less reason to trust that the cybercriminal would provide the videotaped destruction of the exfiltrated data, actually destroy the data, not copy the data, or not sell the data.

⁴ Friedberg Dep. at 135:20-22, 139:9-13.

⁵ Friedberg Dep. at 283:15-23; PX24.

⁶ *Learn more about the ransomware attack we recently stopped*, Blackbaud (July 16, 2020), <https://www.blackbaud.com/newsroom/article/2020/07/16/learn-more-about-the-ransomware-attack-we-recently-stopped> [hereinafter *Learn More Announcement*] [<https://perma.cc/UEF5-ZZ7B>]; PX25.

⁷ Friedberg Dep. at 72:16-73:5; 76:17-24; PX9.

⁸ Friedberg Dep. at 72:16-73:5; PX9.

Unsurprisingly, to date, there is nothing to demonstrate the anonymous cybercriminal did adhere to its promises.

12. The Data Breach, as described herein, is far greater than Blackbaud's belated and inadequate notices have suggested. In fact, cybercriminals demonstrably exfiltrated no less than [REDACTED], constituting [REDACTED] files—an astronomical amount of data.⁹

13. Blackbaud's former Cyber Security Incident Responder, Ricky Banda testified [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
¹⁰ He stated [REDACTED]

¹¹

14. Instead of providing fulsome notice to the individuals who were impacted by the ransomware attack, Blackbaud has downplayed the incident, insisting that, although cybercriminals were able to exfiltrate information from Blackbaud's system, those same criminals can be trusted to have destroyed any copies of the data. But it has been advised [REDACTED]

[REDACTED]¹² Moreover, Blackbaud [REDACTED]
[REDACTED]¹³ This increased the likelihood that the stolen data was published or shared by the initial attacker. As a result, Plaintiffs and Class

⁹ BLKB MDL 00000001 at 12. Blackbaud later [REDACTED]
[REDACTED].

¹⁰ Deposition of Ricky Banda ("Banda Dep.") at 194:13-15, 194:18-21.

¹¹ *Id.* at 194:18-195:2.

¹² Friedberg Dep. at 283:15-23; PX24.

¹³ Friedberg Dep. at 72:16-73:5; 200:6-201:14, 201:24-202:2, 202:5-7; PX9; PX18 at 2.

members are left with empty platitudes instead of vital information that would allow them to take proactive measures to prevent identity theft and future fraud.

15. Blackbaud’s unlawfully deficient data security and utter failure, even now, to honestly address the breach has injured millions of donors, students, and patients, the Plaintiffs and putative Class members in this action. And its false reassurances have coaxed its customers to be less vigilant than they should, violating Blackbaud’s notice obligations.

II. NATURE OF THE ACTION

16. Blackbaud describes itself as “the world’s leading cloud software company powering social good[,]” and claims it “equip[s] change agents with cloud software, services, expertise, and data intelligence designed with unmatched insight and supported with unparalleled commitment.”¹⁴ According to Blackbaud, “[e]very day, [its] customers achieve unmatched impact as they advance their missions.”¹⁵ Furthermore, as it repeatedly represented in investor presentations, “[s]ocial good is a significant global sector.”¹⁶ According to its website, its clients include arts and cultural organizations, companies (conducting corporate social responsibility activities), faith communities, foundations, healthcare organizations, higher education institutions, individual change agents, K-12 schools, and nonprofit organizations (the “Social Good

¹⁴ *Learn More Announcement*, *supra* n.6; PX25.

¹⁵ *Id.*

¹⁶ See, e.g., Investor Presentations dated July 30, 2019 at 6 [<https://perma.cc/88A4-N659>], Oct. 16, 2019 at 8 [<https://perma.cc/YN4N-28S2>], May 5, 2020 at 7 [<https://perma.cc/2ALK-D57M>], July 29, 2020 at 6 [<https://perma.cc/NPR6-UNDP>], Oct. 28, 2020 at 6 [<https://perma.cc/6PVW-4DUP>], Feb. 8, 2021 at 6 [<https://perma.cc/G4HF-9UHB>], and Nov. 3, 2021 at 6 [<https://perma.cc/RJ5Y-HGFY>].

Entities”).¹⁷ Plaintiffs and Class members are the Social Good Entities’ donors, students, patients, and congregants.

17. Blackbaud touts the success of its business: “Blackbaud has grown to serve millions of users across more than 100 countries, including one out of three Fortune 500 companies, 80% of the most influential nonprofits, 30 of the 32 largest nonprofit hospitals, 93% of higher education institutions with billion-dollar campaigns, 25 of the largest Catholic Dioceses in the US and more.”¹⁸

18. Blackbaud has created a profitable business by catering to the needs of Social Good Entities—namely, providing data security services for information that it knows is incredibly valuable. According to Blackbaud’s most recent Form 10-K filed with the Securities and Exchange Commission (“SEC”) on February 23, 2021 (the “2020 Form 10-K”):

Many social good organizations use manual methods or software applications not specifically designed for fundraising and organizational management for institutions like theirs. Such methods are often costly and inefficient because of the difficulties in effectively collecting, sharing and using donation-related information. Furthermore, general purpose software applications frequently have limited functionality for the unique needs of our customer base and do not efficiently integrate multiple databases

* * * * *

Because of these challenges, [Blackbaud] believe[s] nonprofits, education institutions, healthcare organizations and houses of worship can benefit from software applications and services specifically designed to serve their particular needs and workflows to grow revenue, work effectively and accomplish their missions.

¹⁷ *Who We Serve & Industries We Support*, Blackbaud, <https://www.blackbaud.com/who-we-serve> (last visited Dec. 19, 2021) [<https://perma.cc/L4YF-J5QM>].

¹⁸ *Blackbaud CEO Mike Gianoni Named One of 50 Most Influential by Charleston Business Magazine*, Blackbaud (Mar. 12, 2021), <https://www.blackbaud.com/newsroom/article/2021/03/12/blackbaud-ceo-mike-gianoni-named-one-of-50-most-influential-by-charleston-business-magazine> [<https://perma.cc/M8WM-7M9J>].

19. Blackbaud markets itself to Social Good Entities by developing data-hosting “solutions” to meet those entities’ needs; Blackbaud knows that nonprofits devote their resources to fundraising and benefit management and are unable to benefit from the economy of scale afforded by large scale data warehousing and management. Requisite security for such information requires management by a third party specializing in competent management of data, compliant with the representations made to donors, and other obligations by contract, regulation, and statute. As part of its solutions-based services, Blackbaud assured its customers, prior to the discovery of the Data Breach (described further below), that Blackbaud employed “world-class security, privacy, and risk management teams” to ensure the safety of data entrusted to Blackbaud.¹⁹ Blackbaud assured its customers, who entrusted Plaintiffs’ and Class members’ data to Blackbaud, that it had robust cybersecurity practices in place, which are known in the industry as specifically designed to thwart cybercrime like the Data Breach that took place here.²⁰

20. Blackbaud knew that the information it hosted from the Social Good Entities contained some of Class members’ most valuable personal information. Like other entities that host such information, Blackbaud knew that hosting such information made it an attractive target

¹⁹ Security, Blackbaud (Mar. 2, 2020), <https://web.archive.org/web/20200302212750/https://www.blackbaud.com/security>. Throughout this Complaint, Plaintiffs cite to previously-imaged versions of Blackbaud’s and others’ websites. Those images are housed by an independent, third parties called the Internet Archive and Perma.cc. Courts have previously taken judicial notice of web pages available through the Internet Archive’s “WayBack Machine.” See, e.g., *Pohl v. MH Sub I, LLC*, 332 F.R.D. 713, 716 (N.D. Fla. 2019) (collecting cases); see also The Bluebook: A Uniform System of Citation R.18.2.1(d) (Columbia Law Review Ass’n et al. eds., 21st ed. 2020) (encouraging the archiving of internet sources and citing the WayBack Machine and Perma.cc as “reliable” archival tools). Plaintiffs have no reason to doubt the authenticity of the WayBack Machine or Perma.cc’s archives of Blackbaud’s or others’ websites and will obtain evidence confirming their accuracy as the case progresses.

²⁰ *Id.*

for cybercrime, noting that it “may still be vulnerable to a security breach, intrusion, loss or theft of confidential donor data and transaction data[.]”²¹

21. Sophisticated companies like Blackbaud are aware of the different types of threat actors acting across the Internet and the type of security exploits they employ for profit. Accordingly, it is imperative that, as a company that specializes in and profits off of providing data security services to others, it guards against those exploits.

22. One typical type of exploit is called a “ransomware attack,” where an entity uses malicious code to encrypt data on a local machine, demanding a ransom for an encryption key to allow an entity to access the encrypted files again.²²

23. A far more nefarious and dangerous exploit is when a criminal enterprise is able to exfiltrate data from an entity’s systems and demand a payment for that data’s return. Although some describe this type of attack as a “ransomware attack,” as well, the damage is far greater than a typical ransomware attack because the criminal enterprise is in possession of the information, and payment of the demanded ransom (or blackmail) cannot guarantee its destruction.

24. On July 16, 2020, a breaking news story by *The NonProfit Times* reported that Blackbaud had been the subject of a ransomware attack and data breach (the “Data Breach”). Blackbaud claimed it first learned of the Data Breach in May 2020.²³ According to the article, Blackbaud made a demanded blackmail payment to a cybercriminal in an undisclosed amount

²¹ See, e.g., Form 10-K filed with the SEC on February 24, 2016, February 22, 2017, February 20, 2018, February 20, 2019, February 20, 2020, and February 23, 2021.

²² *Ransomware, Scams and Safety, Common Scams and Crimes*, <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware> (last visited Dec. 19, 2021) [<https://perma.cc/33UM-6UQM>].

²³ Paul Colclery, *Breaking: Blackbaud Hacked, Ransom Paid*, NonProfit Times (July 16, 2020), https://www.thenonprofittimes.com/npt_articles/breaking-blackbaud-hacked-ransom-paid [<https://perma.cc/9BCL-8F5X>].

using Bitcoin.²⁴ The victims of the Data Breach were Plaintiffs and Class members. As reported by *The NonProfit Times*, a Blackbaud spokesperson sought to assure consumers that “[c]redit card information, bank account information, or Social Security numbers were not stolen” and that Blackbaud claimed it had “credible information” that the data that was stolen went no further than the cybercriminals.²⁵ On that same day, Blackbaud also issued a statement regarding the Data Breach on its website.²⁶ Despite this, in its 2020 Form 10-K, Blackbaud touted that: “[i]n 2020, [it] showed why [Blackbaud] continue[s] to be the trusted leader in this space.”²⁷ The information that Blackbaud disseminated regarding the Data Breach was misleading and inaccurate in numerous material ways.

25. The release, disclosure, and publication of a person’s sensitive, private data can be devastating. Not only is it an intrusion of privacy and a loss of control, but it is also a harbinger of identity theft: for victims of a data breach, the risk of identity theft more than quadruples.²⁸ A data breach can have grave consequences for victims for many years after the actual date of the breach—with the obtained information, identity thieves can wreak many forms of havoc: open new financial accounts, take out loans, obtain medical services, obtain government benefits, or obtain driver’s licenses in the victims’ names, forcing victims to maintain a constant vigilance over the potential misuse of their information.

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Learn More Announcement*, *supra* n.6; PX25.

²⁷ Blackbaud 2020 Form 10-K.

²⁸ Dave Maxfield & Bill Latham, *Data Breaches: Perspectives from Both Sides of the Wall*, 29-35, 30 S.C. Lawyer (May 2014), <https://mydigitalpublication.com/publication/?m=18928&i=208503&p=1&ver=html5> [<https://perma.cc/L3KT-VQXC>].

26. When information is stolen by cybercriminals, the risk of identity theft does not go away simply because an entity elects to submit to the cybercriminals' demand for a ransom or blackmail payment. If anything, payment of a ransom demonstrates to cybercriminals that the data has value and can continue to be exploited for future payments—not just by the entity from whom the data was stolen, but from the individuals whose data was stolen, themselves.

27. Blackbaud was keenly aware of the risks of cyberattacks and breaches of its customers' confidential data. It knew of the risk because Blackbaud had already suffered a cybersecurity incident in which the laptop belonging to a Blackbaud employee was stolen from the employee's vehicle, *after the employee had copied Private Information from donors onto the device.*²⁹ At the time the breach was reported, Blackbaud insisted that it would "move immediately to do everything we can to help our customers and notify the people whose names and personal information are on those files."³⁰ It took nearly eight months to disclose that the breach also impacted 84,000 University of North Dakota donors.³¹ [REDACTED]

[REDACTED] 32

28. Blackbaud also showed that it knew of the risk it faced by virtue of its own representations. In its Annual Report filed with the SEC, Blackbaud noted that the "secure

²⁹ Identity Theft Resource Center 2008 Breach List (Jan. 2, 2009), https://www.idtheftcenter.org/images/breach/Breach_Report_2008.pdf.

³⁰ Nicole McGougan, Blackbaud: Press Release (Oct. 25, 2008 3:43 PM), <https://www.blackbaud.com/newsroom/article/2008/10/25/blackbaud-press-release> [<https://perma.cc/W9XM-4N6J>].

³¹ (*Update*) ND: Stolen laptop contained donors' financial data, DataBreaches.net (June 17, 2009), <https://www.databreaches.net/update-nd-stolen-laptop-contained-donors-financial-data/> [<https://perma.cc/YPM4-7W8M>].

³² Friedberg Dep. at 33:6-35:8, 105:3-10, 224:5-225:8, 225:15-232:7.

collection, storage, and transmission of confidential” data is fundamental to its business.³³

Blackbaud likewise was aware of the significant risk of cyberattacks, identifying security breaches and theft of confidential donor data as a vulnerability.³⁴ In that same document, Blackbaud also acknowledged its obligation of notification in the event of a breach.³⁵

29. Nevertheless, in February 2020—the same month Blackbaud acknowledged this risk—Blackbaud failed to stop the Data Breach. Blackbaud failed to detect the initial ransomware attack, and for *three and a half months*, between February 7, 2020, and May 20, 2020, cybercriminals orchestrated what Blackbaud has downplayed as a “security incident,” in which they exploited Blackbaud’s inadequately-protected computer networks, gained access to data, and copied data and servers managed, maintained, and secured by Blackbaud.³⁶

30. Blackbaud’s servers contained Personally Identifiable Information (“PII”) and Protected Health Information (“PHI”) (collectively, “Private Information” or “PI”) of individuals, including Plaintiffs and Class members. According to the Federal Trade Commission (“FTC”), PII is “information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.”³⁷ PHI is

³³ Blackbaud, Inc., Annual Report (Form 10-K) (hereinafter “2019 Form 10-K”) at 20 (Feb. 20, 2020), <https://investor.blackbaud.com/static-files/9cd70119-4e13-4d47-b068-3c228c580417>.

³⁴ *Id.*

³⁵ *Id.*

³⁶ Blackbaud, Inc., Form 8-K at 2 (Sept. 29, 2020) [hereinafter Sept. 2020 Form 8-K]. This attack was not a typical “ransomware” attack; the cybercriminals did not encrypt Blackbaud’s environment with malware to extort payment for decryption, as is standard in most ransomware attacks, but rather exfiltrated a copy of data from Blackbaud’s environment and issued a ransom on the exfiltrated data. *See supra* n.6.

³⁷ See *Federal Trade Commission Privacy Impact Assessment: Redress Enforcement Database (RED)* at 3, n.3, FTC (June 2019), https://www.ftc.gov/system/files/attachments/privacy-impact-assessments/redress_enforcement_database_red_privacy_impact_assessment_june_2019.pdf [<https://perma.cc/VM2Z-GC54>].

deemed private under the Healthcare Insurance Portability and Accountability Act of 1996 (“HIPAA”), 42 U.S.C. §§ 1320d, *et seq.*, as well as multiple state statutes. According to the U.S. Department of Health & Human Services (“HHS”), PHI “is information, including demographic data,” that relates to: “the individual’s past, present or future physical or mental health or condition,” “the provision of health care to the individual,” or “the past, present, or future payment for the provision of health care to the individual,” and that “identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.” Individually identifiable health information includes many common identifiers (*e.g.*, name, address, birth date, SSN).”³⁸

31. According to Confidential Witness No. 1, a former information security analyst at Blackbaud, Blackbaud failed to maintain its information on current databases—it failed to heed vendor announcements regarding the sunset of certain databases, leaving client information on older databases that were more vulnerable to cyberattack.

32. Additionally, the [REDACTED]

Instead, Blackbaud discussed internally that [REDACTED]

33. According to Confidential Witness No. 1, his team suggested a year prior to the Data Breach that the data on Blackbaud’s servers needed to be encrypted to reduce vulnerabilities; however, because the servers were so old, the “exact nature of the data was unknown.”

³⁸ See *Summary of the HIPAA Privacy Rule*, HHS, <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (last visited Dec. 19, 2021) [<https://perma.cc/77KL-PC46>].

34. While most information about the Data Breach remains fuzzy given Blackbaud’s failure to disclose the full details of its investigation of the breach to the public—including how many entities were impacted by the Breach—the sources of the information largely fall into three categories:

Healthcare Information	Educational Information	Information from Nonprofits and NGOs
Healthcare organizations across the globe use Blackbaud as their cloud software company. Most of the information impacted appears to be donor information; however, a significant number of notices have been sent to patients concerning exposure of PHI.	Blackbaud offers management software to K-12 schools, as well as universities. Some of the management software includes student information, learning management, enrollment management, and school websites. Most of the information impacted appears to be donor information, alumni information, student I.D. numbers, and student demographic information.	Nonprofits appear to be the largest users of Blackbaud’s services. Blackbaud offers an array of software services that cater to nonprofits worldwide, but is best known for its customer relationship management (“CRM”) tools. Many nonprofits use CRMs to nurture donor relationships and fundraise.

35. As a result of this Data Breach, Plaintiffs and millions of Class members have suffered and will continue to suffer concrete and actual harm.³⁹ Plaintiffs’ and the Class members’ sensitive Private Information—which was entrusted to Blackbaud over the course of several years through the Social Good Entities, including educational institutions, hospital and healthcare systems, religious organizations, and charitable institutions—was compromised and unlawfully accessed as a result of the Data Breach and made subject to unlawful use by cybercriminals.

36. The cybercriminals who committed the Data Breach understand that the stolen data has value—Blackbaud has already paid a ransom to ensure its alleged destruction. But criminals

³⁹ Jessica Davis, *Blackbaud Confirms Hackers Stole Some SSNs, As Lawsuits Increase*, HealthITSecurity (Sept. 30, 2020), <https://healthitsecurity.com/news/blackbaud-confirms-hackers-stole-some-ssns-as-lawsuits-increase> [https://perma.cc/X2HP-VT7Y].

have no incentive to destroy such valuable information that may be monetized in the future, either through extracting additional ransom payments (from either Blackbaud or the individual consumers affected), or using the data to commit fraud and identity theft. As cybersecurity professional Brian Krebs has noted:

Companies hit by ransomware often face a dual threat: Even if they avoid paying the ransom and can restore things from scratch, about half the time the attackers also threaten to release sensitive stolen data unless the victim pays for a promise to have the data deleted. Leaving aside the notion that victims might have any real expectation the attackers will actually destroy the stolen data, new research suggests a fair number of victims who do pay up may see some or all of the stolen data published anyway.⁴⁰

37. Blackbaud continues to tout the fact that it acquiesced to the cybercriminals' extortion demands as a success, noting that the payment "prevented the cybercriminal from blocking our system access and fully encrypting files," and somehow guaranteed that information that was stolen from Blackbaud's servers had been deleted.⁴¹ However, as explained below,

[REDACTED]

[REDACTED]

[REDACTED]

38. Accordingly, and against professional guidance from cybersecurity professionals to the contrary, Blackbaud assumes that it has "no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly."⁴²

⁴⁰ Krebs, *supra* n.1.

⁴¹ Blackbaud, *supra* n.6.

⁴² *Id.*

39. Blackbaud refuses to provide detailed information, leaving consumers to fill in the blanks. They are forced to simply rely upon notices of the Data Breach from entities that contracted with Blackbaud to host the data (“Notices”), which are just as confused. As a result, and because Blackbaud has refused to provide consumers with basic information that they could use to protect themselves and take specific, preventative measures, Plaintiffs and Class members incurred out-of-pocket costs, including the cost of identity theft protection and insurance services, as well as time spent on taking preventative measures and responding to actual incidents of identity theft and fraud.

40. Despite knowing the devastating reach of the Data Breach, Blackbaud continues to misrepresent the extent of the breach on its website.⁴³ Contrary to Blackbaud’s continued representations, as reflected in its statement related to the Data Breach and the Notices that Plaintiffs received, credit card numbers, bank account numbers, and/or other Private Information were compromised.

41. Despite Blackbaud’s prior representations to the contrary, the public is now able to cobble together that that information compromised in the Data Breach included at least the following categories of Private Information:

- a. Personal identifiers, including full name, title, age, date of birth, and SSNs;
- b. Contact information, including addresses, phone numbers, email addresses, and LinkedIn profiles;
- c. Financial information, including bank account information, estimated wealth, identified assets, donation histories, values of donations, and donation recipient organizations;
- d. Medical and health information, including patient and medical record identifiers, treating physician names, medical visit dates, reasons for

⁴³ *Security Incident*, Blackbaud (updated Sept. 29, 2020), <https://www.blackbaud.com/securityincident> [https://perma.cc/3HHD-4TD8].

- seeking medical treatment, patient discharge statuses, and health insurance status (*i.e.*, PHI);
- e. Demographic information, including gender, political opinions, and religious beliefs;
 - f. Account credentials, including usernames and passwords;
 - g. Employment information, including employers, hire dates, annual salaries, and payroll amounts;
 - h. Marital details, including marital statuses, spouse names, and spouses' giving histories; and
 - i. Educational information, including student ID numbers, course and educational attainment details.⁴⁴

⁴⁴ Form 8-K, *supra* n.36; Leo Kelion & Joe Tidy, *National Trust Joins Victims of Blackbaud Hack*, BBC News (July 30, 2020), <https://www.bbc.com/news/technology-53567699> [<https://perma.cc/VQ3R-VW8N>]; *Blackbaud Security Breach and How It Affects You, Your Privacy and Big Thought*, Big Thought, <https://www.bigthought.org/announcements/news-announcements/blackbaud-security-breach-and-how-it-affects-you-your-privacy-and-big-thought/> (last visited Dec. 19, 2021) (“In addition, for individuals employed by Big Thought from July 15, 2008 through March 31, 2010, birth date, gender, marital status, hire date, bank name, annual salary and payroll amounts may have been accessed despite being encrypted.”) [<https://perma.cc/4AM4-MAR4>]; *Notice to Our Patients of a Privacy Incident*, White Plains Hospital. (Sept. 30, 2020), <https://www.wphospital.org/getmedia/71a84f33-91f4-433b-b34f-116113bed5a2/White-Plains-Substitute-Notice-Draft-FINAL> (“Based on White Plains Hospital’s review of the Blackbaud database involved in the incident, it contained some patient information, including names, addresses, dates of birth, patient identifiers, and potentially in some instances, treating physician names, visit dates, and/or reasons for seeking treatment.”) [<https://perma.cc/Z8XX-NF24>]; *Blackbaud Security Incident*, Children’s Minnesota (Sept. 11, 2020), <https://www.childrensmn.org/2020/09/11/blackbaud-security-incident/> (“Based on our investigation and review of the affected Blackbaud database, the incident involved limited patient information that the Foundation received in connection with its fundraising efforts, including: full names, addresses, phone numbers, age, dates of birth, gender, medical record numbers, dates of treatment, locations of treatment, names of treating clinicians and health insurance status.”) [<https://perma.cc/7JEB-2Q3G>]; *Blackbaud Response*, Univ. of York (July 21, 2020), <https://www.york.ac.uk/news-and-events/news/2020/blackbaud-response/> (“The data accessed by the cybercriminal may have contained some of the following information: Basic details, [e.g.,] name, title, gender, date of birth and student number (if applicable); Addresses and contact details, [e.g.,] phone, email and LinkedIn profile URL; Course and educational attainment details, [e.g.,] what qualification you received and some of the extracurricular opportunities you participated in while studying at York (if applicable”)] [<https://perma.cc/P9YB-GDY4>]; *Blackbaud Security Incident: What information was accessed by the criminals?*, Mercy Hosp. & Med. Ctr., <http://www.mercy-chicago.org/blackbaud-security-incident> (last visited Dec. 19, 2021) (“Other fields were not encrypted and could have been accessible to the cybercriminals including

42. Had Blackbaud maintained a sufficient security program, including properly monitoring its network, security, and communications, it would have discovered the cyberattack sooner or prevented it altogether. In fact, Blackbaud has announced it has “already implemented changes to prevent this specific issue from happening again.”⁴⁵ Had the necessary changes been made previously, this incident would not have happened, and Plaintiffs’ Private Information would not have been accessed.

43. Plaintiffs’ Private Information has been compromised and disclosed to unauthorized third parties because of Blackbaud’s negligent and unlawful conduct—the Private Information that Blackbaud collected and maintained is now in the hands of cybercriminals. Blackbaud cannot reasonably maintain that the data thieves destroyed the extracted data simply because Blackbaud paid the ransom and the perpetrators stated the copy was destroyed. In fact, the Notices provided by the non-profit organizations and educational and other institutions through which Blackbaud obtained Plaintiffs’ data advised that Plaintiffs and Class members should remain aware of suspicious account activity, take further actions such as monitoring their own credit records, and notify the organizations involved and law enforcement authorities of any suspicious activity.⁴⁶ Despite this, Blackbaud offered Class members little in the way of redress,

information such as: donor relation to patient, patient discharge status, name of patient insurance and patient department of service, your name, contact information, donation history.”).

⁴⁵ *Id.*

⁴⁶ For instance, the notice provided to Plaintiff Jessica Case warned that she should “remain vigilant and promptly report any suspicious activity or suspected identity theft to [the non-profit] and to the proper law enforcement authorities, such as the Federal Trade Commission and the Washington State Office of the Attorney General.” Likewise, the notice Plaintiff Kea Molnar received advised her to “remain vigilant and promptly report to [the educational institution] and to the proper law enforcement authorities any suspicious activity or suspected identity theft.”

such as credit monitoring or fraud protection, and provided no financial support for time or expenses incurred as a result of the Data Breach.

44. In response to some of the most egregious instances of stolen data from the Data Breach, Blackbaud has provided minimal support—an offer of two years of single-bureau credit monitoring and “access remediation support” from CyberScout Fraud Investigator for only those individuals who had their most sensitive PII taken in unencrypted form, such as SSNs.⁴⁷ Some Social Good Entities have also offered identity theft protection services. But those services, standing by themselves, are plainly inadequate: single-bureau monitoring “leaves too much to chance,”⁴⁸ and the cybersecurity criminals who stole the data from Blackbaud’s systems will likely attempt to monetize it again.⁴⁹ Consequently, Plaintiffs and Class members have incurred and will incur out of pocket costs for purchasing their own credit monitoring services or credit reports, or spending money or time on other protective measures as a reasonable solution to deter and detect identity theft.

45. Cybersecurity criminals can also use this data to demand further ransoms from the individuals whose Private Information was stolen off of Blackbaud’s servers. Since Blackbaud already demonstrated to the cybercriminals that the data is valuable enough to extract a ransom,

⁴⁷ In Blackbaud’s letter dated September 29, 2020 to the Kushner School, Blackbaud offered “Identity Theft Protection services to individuals whose Social Security Numbers … are stored in the areas we described above at no cost to you or the individuals.” Cleve Warren, Executive Director of FSCJ, described that on September 29, 2020, Blackbaud informed the FSCJ Foundation that a back-up file was taken in the ransomware attack and that it contained “certain information that was part of a legacy table of names and Social Security numbers retained on Blackbaud servers that was not encrypted.” <https://www.fscjfoundation.org/Blackbaud.html> (last visited Dec. 19, 2021) [<https://perma.cc/78T9-VYFE>].

⁴⁸ *Should I monitor my credit with one credit bureau or all three? Why it’s better to be thorough if you want to guarantee the best credit possible*, Debt.com (Oct. 28, 2020), <https://www.debt.com/credit-monitoring/three-credit-bureaus/>.

⁴⁹ Krebs, *supra* n.1.

Plaintiffs and Class members face an imminent risk of future harm of paying cybercriminals to protect their information from further disclosure based upon new ransom threats for the same information.⁵⁰

46. As a result of the Data Breach, Plaintiffs and the Class members have suffered concrete damages and are now exposed to a heightened and imminent risk of fraud, identity theft, and ransom demands for many years to come. Furthermore, Plaintiffs and Class members must now and in the future closely monitor their financial accounts to guard against identity theft at their own expense. Consequently, Plaintiffs and the Class members will incur ongoing out-of-pocket costs including the cost of credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft, among other expenses.

47. By this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was compromised and disclosed as a result of the Data Breach.

48. Accordingly, Plaintiffs bring this action against Blackbaud seeking redress for its unlawful conduct, and asserting claims for both common law and statutory damages.

III. PARTIES

A. Plaintiffs

49. Plaintiffs identified below bring this action on behalf of themselves and those similarly situated in a representative capacity for individuals across the United States. Despite knowing of the substantial cybersecurity risks it faced, Blackbaud, through its actions described herein, leaked, disbursed, and furnished Plaintiffs' valuable Private Information to unknown

⁵⁰ See *Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues, Coveware* (Nov. 4, 2020), <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report> [<https://perma.cc/6ABQ-DVE3>].

cybercriminals, thus causing them present, immediate, imminent, and continuing increased risk of harm.

50. As used throughout this Complaint and previously defined in paragraph 30, “Private Information” is further defined as all information exposed by the Data Breach, including all or any part or combination of name, address, birth date, SSN, PHI, driver’s license information (including license number, state, home address, dates of issuance or expiration), telephone number, email address, tax identification number, credit card number, or dispute documents with PII (such as images of government-issued identifications).

ALABAMA

51. Based upon counsel’s investigation, and upon information and belief, residents and citizens of the State of Alabama were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Alabama.

ALASKA

52. Based upon counsel’s investigation, and upon information and belief, residents and citizens of the State of Alaska were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Alaska.

ARIZONA

53. Based upon counsel’s investigation, and upon information and belief, residents and citizens of the State of Arizona were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Arizona.

ARKANSAS

54. Based upon counsel’s investigation, and upon information and belief, residents and citizens of the State of Arkansas were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Arkansas.

CALIFORNIA

55. Plaintiff **Kassandre Clayton** is a resident and citizen of California. Plaintiff Clayton is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Clayton's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Clayton would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Clayton's Private Information was compromised and disclosed as a result of the Data Breach.

56. Plaintiff Clayton was required to provide her PHI to several healthcare providers as a predicate to receiving healthcare services. Plaintiff Clayton's PHI was in turn provided to Blackbaud to be held for safekeeping. In or around September 2020, Plaintiff Clayton received notice from Community Medical Centers that her PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Clayton's PHI, including, her name, address, phone number, email address, date of birth, room number, patient identification number, name of hospital where treated, applicable hospital department or unit had been improperly accessed and/or obtained by unauthorized third parties. Additionally, she received notice from Trinity Health that her name, address, phone number, email, most recent donation date, date of birth, age, inpatient/outpatient status, dates of service, hospital location, patient room number and physician name were compromised as a result of the Data Breach.

57. While the notices indicated that the Data Breach did not involve the exposure of credit card information, bank account information, SSNs and any additional medical information, such as diagnosis or treatment plan and/or that certain categories of data were encrypted, later forensic investigations have revealed that Blackbaud's representations about what information was

exposed and/or encrypted, including SSNs, were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Clayton's was exposed due to Blackbaud's conduct.

58. As a result of the Data Breach, Plaintiff Clayton tried to mitigate its impact after receiving the notification letters, including 2 hours of time spent reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud, and between 1 and 2 hours monitoring online banking to resolve issues related to the Data Breach. Plaintiff Clayton now spends approximately 3 hours per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least 15-20 hours on these tasks, valuable time Plaintiff Clayton otherwise would have spent on other activities, including but not limited to work and/or recreation.

59. Since Plaintiff Clayton was not offered credit monitoring and identity theft protection services by Blackbaud, in an effort to mitigate its impact after receiving the notification letters, she purchased and continues to maintain credit monitoring. Upon receiving notification of the Data Breach, Plaintiff Clayton purchased credit monitoring and identity theft protection services on an annual basis for approximately \$189.95 per year from IdentityProtection.com beginning October 7, 2020. Plaintiff Clayton plans to continue purchasing credit monitoring and identity theft protection services on an ongoing basis to protect herself from identity theft and fraud.

60. As a result of the Data Breach, Plaintiff Clayton has suffered emotional distress as a result of the release of her Private Information and PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff

Clayton is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

61. Plaintiff Clayton suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Blackbaud obtained from Plaintiff Clayton; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

62. Moreover, subsequent to the Data Breach, Plaintiff Clayton also experienced actual identity theft and fraud, including notification that her Private Information was found on the dark web and a significantly increased amount of suspicious, unsolicited phishing telephone calls, text messages, and/or emails.

63. Plaintiff Clayton incurred approximately 10 to 15 hours to date, and at least \$189.50 responding to these incidents of attempted identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Clayton otherwise would have spent on other activities, such as work and/or recreation.

64. As a result of the Data Breach, Plaintiff Clayton anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Clayton will continue to be at increased risk of identity theft and fraud for years to come.

65. Plaintiff **Philip Eisen** is a resident and citizen of California. Plaintiff Eisen is acting on his own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Eisen's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Eisen would not have

entrusted his Private Information to one or more Social Good Entities had he known that one of the entity's primary cloud computing vendors entrusted with his Private Information failed to maintain adequate data security. Plaintiff Eisen's Private Information was compromised and disclosed as a result of the Data Breach.

66. Plaintiff Eisen was required to provide his PII to entities to whom he regularly made charitable donations. Plaintiff Eisen's PII was in turn provided to Blackbaud to be held for safekeeping.

67. In or around July 2020, Plaintiff Eisen received notice from Planned Parenthood that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Eisen's PII, including street addresses and telephone number, was compromised as a result of the Data Breach.

68. This notice further indicated that the Data Breach did not involve sensitive data—such as SSNs, credit card data, or bank account information. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus, at this time, it is unclear how much Private Information of Plaintiff Eisen was exposed due to Blackbaud's conduct.

69. As a result of the Data Breach, Plaintiff Eisen made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: researching the Data Breach and Blackbaud; reviewing credit reports, financial account statements; researching credit monitoring and identity theft protection services. Plaintiff Eisen now spends approximately 2 hours per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least 12 hours on these tasks, valuable time Plaintiff

Eisen otherwise would have spent on other activities, including but not limited to work and/or recreation.

70. Since Plaintiff Eisen was not offered credit monitoring and identity theft protection services by Blackbaud, Plaintiff purchased identity theft protection from AAA ProtectMyID.

71. As a result of the Data Breach, Plaintiff Eisen has suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Eisen is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

72. Plaintiff Eisen suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Blackbaud obtained from Plaintiff Eisen; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

73. Moreover, subsequent to the Data Breach, Plaintiff Eisen also experienced actual identity theft and fraud, including notifications that his email address and passwords have been compromised, and a significant increase in suspicious, unsolicited phishing telephone calls and text messages. Plaintiff Eisen has spent approximately 3 hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Eisen otherwise would have spent on other activities, such as work and/or recreation.

74. As a result of the Data Breach, Plaintiff Eisen anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data

Breach. As a result of the Data Breach, Plaintiff Eisen will continue to be at increased risk of identity theft and fraud for years to come.

75. Plaintiff **Mamie Estes** is a resident and citizen of California. Plaintiff Estes is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Estes's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Estes would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Estes's Private Information was compromised and disclosed as a result of the Data Breach.

76. In or around August 2020, Plaintiff Estes received notice from Crystal Stairs, Inc. that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. This letter indicated that Plaintiff Estes's Private Information, including her name, SSN, and/or tax identification number was compromised as a result of the Data Breach.

77. As a result of the Data Breach, Plaintiff Estes made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to, purchasing and continuing to maintain credit monitoring. Further, Plaintiff Estes tried to mitigate the impact of the Data Breach by checking each of her accounts in search of fraudulent charges for at least 10 minutes a day since the Data Breach. Plaintiff Estes now spends approximately 5 hours per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least 10-15 hours on these tasks, valuable time Plaintiff Estes otherwise would have spent on other activities, including but not limited to work and/or recreation.

78. While the notice letter did not indicate the exposure of credit card information, bank account information, and any additional categories of data that were encrypted, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Estes's was exposed due to Blackbaud's conduct.

79. While Plaintiff Estes was offered credit monitoring and identity theft protection services by Blackbaud, through Crystal Stairs, Inc., Plaintiff Estes had already been receiving credit monitoring from Credit Karma. However, after the breach, she also signed up for Experian's Identity Theft plan to receive credit monitoring and identity theft protection services on an ongoing basis to protect herself from identity theft and fraud. Thus, by the time Blackbaud's offer came in, she felt it unnecessary to accept.

80. As a result of the Data Breach, Plaintiff Estes has suffered emotional distress as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Estes is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

81. Plaintiff Estes suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Blackbaud obtained from Plaintiff Estes; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

82. Moreover, subsequent to the Data Breach, Plaintiff Estes also experienced actual identity theft and fraud attempts, including notifications from Experian and Credit Karma that people are attempting to access her accounts on platforms including Amazon, PayPal and Apple. Plaintiff Estes has also received texts and mails from Wells Fargo regarding a checking account that is not hers, because she does not bank with them nor ever has. Plaintiff reasonably believes these activities are related to the Data Breach, since they began last year after the Data Breach, and they continue to occur. In addition, she has begun to receive spam phone calls every day since last year after the Data Breach. In response, she has had to install a call filter that blocks the spam calls.

83. Plaintiff Estes spent approximately 10 to 15 hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Estes otherwise would have spent on other activities, such as work and/or recreation.

84. As a result of the Data Breach, Plaintiff Estes anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Estes will continue to be at increased risk of identity theft and fraud for years to come.

COLORADO

85. Plaintiff **Alexandra L. Mitchell** is a resident and citizen of Colorado. Plaintiff Mitchell is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Mitchell's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Mitchell would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private

Information failed to maintain adequate data security. Plaintiff Mitchell's Private Information was compromised and disclosed as a result of the Data Breach.

86. Plaintiff Mitchell was required to provide her PII as a student at St. Andrew's Episcopal School from on or around 2001 through 2014. Plaintiff Mitchell's PII was in turn provided to Blackbaud to be held for safekeeping. This PII included her name, address, phone number, email address, date of birth, and SSN.

87. In or around December 8, 2020, Plaintiff Mitchell received notice from St. Andrew's Episcopal School that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Mitchell's Private Information, including her name, address, phone number, email address, date of birth, and SSN was compromised as a result of the Data Breach.

88. While the notice letter did not specifically indicate the exposure of credit card information, bank account information, or any additional categories of data, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Mitchell's was exposed due to Blackbaud's conduct.

89. As a result of the Data Breach, Plaintiff Mitchell made reasonable efforts to mitigate its impact after receiving the notification letter, including 5-6 hours of time spent researching the Data Breach and Blackbaud; reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud; researching and enrolling in the credit monitoring and identity theft protection services offered by Blackbaud. To date, Plaintiff Mitchell has spent at least 5-6 hours as a result of the Data Breach, and notes that she has been especially worried she has not had the time yet for more. Nevertheless, this is valuable

time Plaintiff Mitchell otherwise would have spent on other activities, including but not limited to work, school and/or recreation.

90. As a result of the Data Breach, Plaintiff Mitchell has suffered emotional distress as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety and stress about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. She worries daily about her stolen data and how it is being used. She is upset with the lack of protection of her data and identity. She is concerned health records or other personal identifiers may also have been compromised in the breach of her school records. Plaintiff Mitchell is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

91. Plaintiff Mitchell suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Blackbaud obtained from Plaintiff Mitchell; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

92. As a result of the Data Breach, Plaintiff Mitchell anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Mitchell will continue to be at increased risk of identity theft and fraud for years to come.

CONNECTICUT

93. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Connecticut were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Connecticut.

DELAWARE

94. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Delaware were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Delaware.

DISTRICT OF COLUMBIA

95. Based upon counsel's investigation, and upon information and belief, residents and citizens of the District of Columbia were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of the District of Columbia.

FLORIDA

96. Plaintiff **William Carpenella** is a resident and citizen of Florida. Plaintiff Carpenella is acting on his own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Carpenella's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Carpenella would not have entrusted his Private Information to one or more Social Good Entities had he known that one of the entity's primary cloud computing vendors entrusted with his Private Information failed to maintain adequate data security. Plaintiff Carpenella's Private Information was compromised and disclosed as a result of the Data Breach.

97. In or around October 2020, Plaintiff Carpenella received notice by mail from Stetson University that his Private Information had been improperly accessed and/or obtained by unauthorized third parties. The notice indicated that Plaintiff Carpenella's PII, including name, SSN, date of birth, Student ID, demographic information, and philanthropic giving history, such as donation dates and amount, was compromised as a result of the Data Breach.

98. As a result of the Data Breach, Plaintiff Carpenella made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to, continuing

to maintain and pay for credit monitoring. Specifically, Plaintiff spent three to four hours initially, then one hour daily through December 2020, and then two hours per week from January 2021 to March 2021, reviewing his credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud, researching and enrolling in the credit monitoring and identity theft protection services, and researching and purchasing credit monitoring and identity theft protection services. Plaintiff Carpenella also spent four hours on the phone with his bank trying to establish a new auto loan and home equity line of credit at the time he was notified of the Data Breach. In addition, Plaintiff Carpenella now spends approximately eight hours per month reviewing his credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff estimates that he has spent at least 100 hours on these tasks, valuable time Plaintiff Carpenella otherwise would have spent on other activities, including but not limited to work and/or recreation.

99. While the notice did not specifically indicate the exposure of Plaintiff Carpenella's credit card information, bank account information, SSN, or additional categories of data, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate and/or incomplete at best. Thus, at this time, it is unclear how much Private Information of Plaintiff Carpenella was exposed due to Blackbaud's conduct.

100. As a result of the Data Breach, Plaintiff Carpenella has suffered emotional distress, including anxiety tied to the thought of unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Carpenella, who reasonably expected that his Private Information would be protected, is very concerned about the imminent risks of identity theft and fraud attendant to the Data Breach. He has worked very hard to achieve

a near-perfect credit rating and is extremely worried about it being affected by the exposure of his Private Information in the Data Breach. Further, Plaintiff Carpenella has been attempting to get a Home Equity Line of Credit to pay for updates to his home and reasonably believes he is at imminent risk that the Data Breach will cause his calculated and time-intensive efforts to fall through.

101. As a result of his Private Information being compromised in the Data Breach, Plaintiff Carpenella has suffered injury, including, but not limited to: (a) damage to and diminution in the value of his Private Information, a form of property that Blackbaud obtained from Plaintiff Carpenella; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

102. Moreover, following the Data Breach, Plaintiff Carpenella has received indications that he is at actual risks of identity theft and fraud, including dark web notifications from his credit monitoring service and an increase in the number of spam phone calls. Specifically, Plaintiff Carpenella now receives over ten calls per day for warranties, home refinance, and other solicitations. Prior to the Data Breach, Plaintiff Carpenella did not receive these types of calls.

103. Plaintiff Carpenella incurred approximately 100 hours responding to these incidents of identity theft and fraud as a result of the Data Breach. As a result of the Data Breach, Plaintiff Carpenella has made it a point to continuously check his credit score, via his personal American Express CREDITSECURE account, and spent time checking and removing a large inflow of junk mail regarding credit applications, mortgage refinancing and other matters.

104. As a result of the Data Breach, Plaintiff Carpenella anticipates that his efforts to mitigate and address the harms caused by the Data Breach will be ongoing, including spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by

the Data Breach. As a result of the Data Breach, Plaintiff Carpenella continues to be at an increased risk of identity theft and fraud.

105. Plaintiff **Dorothy Kamm** is a resident and citizen of Florida. Plaintiff Kamm is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Kamm's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Kamm would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Kamm's Private Information was compromised and disclosed as a result of the Data Breach.

106. Plaintiff Kamm was required to provide her PII to certain organizations as a prerequisite to giving donations and signing up for rewards programs. Plaintiff Kamm's PII was in turn provided to Blackbaud to be held for safekeeping. These organizations included; The Cornell Lab of Ornithology (August 2020), Archbold Biological Station (August 2020), and Planned Parenthood (August 2020). Plaintiff Kamm's PII was exposed as a direct and proximate result of the Data Breach from each of these organizations.

107. Each of the notices received by Plaintiff Kamm from the four organizations notified her of the Data breach, the exposure of her PII and suggestions of how to protect herself. The notices further indicated that the Data Breach did not involve the exposure of credit card information, bank account information, SSNs and any additional categories of data that were encrypted. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best.

Thus at this time, it is unclear how much Private Information of Plaintiff Kamm's was exposed due to the Data Breach.

108. As a result of the Data Breach, Plaintiff Kamm tried to mitigate its impact after receiving the notification letter, including at least 2 hours responding to the Data Breach involving Blackbaud. To date, Plaintiff has spent at least 2 hours on these tasks, valuable time Plaintiff Kamm otherwise would have spent on other activities, including but not limited to work and/or recreation.

109. As a result of the Data Breach, Plaintiff Kamm has suffered emotional distress and annoyance as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including worry about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud.

110. Plaintiff Kamm suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Blackbaud obtained from Plaintiff Kamm; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

111. Moreover, subsequent to the Data Breach, Plaintiff Kamm also experienced a significantly increased amount of suspicious, unsolicited phishing telephone calls, text messages, and/or emails.

112. Plaintiff Kamm incurred several hours responding to these incidents of phishing as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Kamm otherwise would have spent on other activities, such as work and/or recreation.

113. As a result of the Data Breach, Plaintiff Kamm anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Kamm will continue to be at increased risk of identity theft and fraud for years to come.

GEORGIA

114. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Georgia were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Georgia.

HAWAII

115. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Hawaii were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Hawaii.

IDAHO

116. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Idaho were impacted by the Data Breach. The other Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Idaho.

ILLINOIS

117. Plaintiff **Kathleen Arman** is a resident and citizen of Illinois. Plaintiff Arman is acting on her own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Arman's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Arman would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed

to maintain adequate data security. Plaintiff Arman's Private Information was compromised and disclosed as a result of the Data Breach.

118. Plaintiff Arman was required to provide her PHI to her healthcare provider as a predicate to receiving healthcare services. Plaintiff Arman's PHI was in turn provided to Defendant to be held for safekeeping.

119. In or around September 2020, Plaintiff Arman received notice from NorthShore University Health System ("NorthShore") that her PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Arman's PHI, including full name, date of birth contact information (address, phone number, email address), admission and discharge date(s), NorthShore location(s) of services, and physician name(s) and specialties, was compromised as a result of the Data Breach.

120. This notice further indicated that the Data Breach did not involve the exposure of credit card, bank account information, SSNs, user login credentials and passwords. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Arman's was exposed due to Blackbaud's conduct.

121. As a result of the Data Breach, Plaintiff Arman made reasonable efforts to mitigate its impact receiving the notification letter, including but not limited to: researching the Data Breach and Blackbaud; reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud and freezing her credit. Plaintiff Arman now spends approximately two hours per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least 16 hours on these

tasks, valuable time Plaintiff Arman otherwise would have spent on other activities, including but not limited to work and/or recreation.

122. Plaintiff Arman was not offered credit monitoring and identity theft protection services by Blackbaud.

123. As a result of the Data Breach, Plaintiff Arman has suffered emotional distress as a result of the release of her PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PHI for purposes of identity theft and fraud. Plaintiff Arman is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

124. Plaintiff Arman suffered actual injury from having her PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PHI, a form of property that Blackbaud obtained from Plaintiff Arman; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

125. Moreover, subsequent to the Data Breach, Plaintiff Arman also experienced actual identity theft and fraud, including notification that her Private Information was found on the dark web and a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or emails. Plaintiff Arman has spent over 20 hours of her time responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with this incident resulting from the Data Breach is time Plaintiff Arman otherwise would have spent on other activities, such as work and/or recreation.

126. As a result of the Data Breach, Plaintiff Arman anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data

Breach. Plaintiff Arman will continue to be at increased risk of identity theft and fraud for years to come.

127. Plaintiff **Helen Lofton** is a resident and citizen of Illinois. Plaintiff Lofton is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Lofton's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Lofton would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Lofton's Private Information was compromised and disclosed as a result of the Data Breach.

128. Plaintiff Lofton was required to provide her PHI to Northwestern Memorial HealthCare, her healthcare provider, as a predicate to receiving healthcare services. Plaintiff Lofton's PHI was in turn provided to Blackbaud to be held for safekeeping. This PHI included name, date of birth, address, gender, and Northwestern Memorial Healthcare medical record number.

129. In or around August 25, 2020, Plaintiff Lofton received notice from Northwestern Memorial HealthCare that her PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Lofton's PHI, including name, date of birth, address, gender, and Northwestern Memorial HealthCare medical record number was compromised as a result of the Data Breach.

130. While the notice indicated that the Data Breach did not involve the exposure of her SSN, payment card or financial account information, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including

SSNs, were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Lofton's was exposed due to Blackbaud's conduct.

131. As a result of the Data Breach, Plaintiff tried to mitigate its impact after receiving the notification letter, including 1 hour researching the Data Breach and Blackbaud and resetting automatic billing instructions tied to compromised accounts. To date, she has spent at least 12 hours on these tasks, valuable time Plaintiff Lofton otherwise would have spent on other activities, including but not limited to work and/or recreation.

132. As a result of the Data Breach, Plaintiff Lofton has suffered emotional distress as a result of the release of her Private Information, including PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Lofton is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach, and is in "panic mode" about the unauthorized disclosure of her Private Information.

133. Plaintiff Lofton suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Blackbaud obtained from Plaintiff Lofton; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

134. Moreover, subsequent to the Data Breach, Plaintiff Lofton also experienced actual identity theft and fraud, including an unauthorized financial charge that she spent considerable time challenging and seeking reimbursement from her institution.

135. Plaintiff Lofton incurred approximately one hour responding to the incident of identity theft and fraud as a result of the Data Breach. The time spent dealing with the incident resulting from the Data Breach is time Plaintiff Lofton otherwise would have spent on other activities, such as work and/or recreation.

136. As a result of the Data Breach, Plaintiff Lofton anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Lofton will continue to be at increased risk of identity theft and fraud for years to come.

INDIANA

137. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Indiana were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Indiana.

IOWA

138. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Iowa were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Iowa.

KANSAS

139. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Kansas were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Kansas.

KENTUCKY

140. Based upon counsel's investigation, and upon information and belief, residents and citizens of the Commonwealth of Kentucky were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Kentucky.

LOUISIANA

141. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Louisiana were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Louisiana.

MAINE

142. Plaintiff **Catharine Gignac** is a resident and citizen of Maine. Plaintiff Gignac is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Gignac's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Gignac would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Gignac's Private Information was compromised and disclosed as a result of the Data Breach.

143. Plaintiff Gignac was required to provide her PHI to her healthcare provider, Eastern Maine Healthcare Systems, d/b/a/ Northern Light, as a predicate to receiving healthcare services. Plaintiff Gignac's PHI was in turn provided to Blackbaud to be held for safekeeping. This PHI included her name, address, phone number, email address, date of birth, gender, the Northern Light hospital at which she received treatment, and likely the departments where she has received medical care and the associated dates of service.

144. In or around September 2020, Plaintiff Gignac received notice from Northern Light that her PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Gignac's name, address, phone number, email address, date of birth, gender, Northern Light Hospital(s) and possibly the departments where she has received medical care and the associated dates of service, were compromised as a result of the Data Breach.

145. This notice indicated that the Data Breach did not involve the exposure of credit card or bank account information. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Gignac's was exposed due to the Data Breach.

146. As a result of the Data Breach, Plaintiff tried to mitigate its impact after receiving the notification letter, including expending approximately 26 hours researching the Data Breach and Blackbaud and reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud. Plaintiff Gignac now spends approximately 4 to 5 hours per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff Gignac has spent at least 26 hours on these tasks, valuable time Plaintiff Gignac otherwise would have spent on other activities, including but not limited to work and/or recreation.

147. Since Plaintiff Gignac was not offered credit monitoring and identity theft protection services by Blackbaud, Plaintiff Gignac has purchased credit monitoring and identity theft protection services on an annual basis for approximately \$120 per year. Plaintiff Gignac plans to continue purchasing credit monitoring and identity theft protection services on an ongoing basis to protect herself from identity theft and fraud.

148. As a result of the Data Breach, Plaintiff Gignac has suffered emotional distress as a result of the release of her Private Information, including PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Gignac is very concerned about identity theft and fraud, as well as the consequences such

identity theft and fraud resulting from the Data Breach may have on her credit score, in particular, which she had concerns about prior to the Data Breach.

149. Plaintiff Gignac suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Blackbaud obtained from Plaintiff Gignac; (b) violation of her privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) actual out of pocket expenditures for credit monitoring.

150. Moreover, subsequent to the Data Breach, Plaintiff Gignac also received an identity theft and fraud notification that her Private Information was found on the dark web, experienced unauthorized attempted changes to her passwords on her social media accounts, a notification from Wells Fargo about issues with an account which she never opened, and a significantly increased amount of suspicious, unsolicited phishing telephone calls, text messages, and/or emails.

151. Plaintiff Gignac incurred approximately 26 hours and \$120 responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Gignac otherwise would have spent on other activities, such as work and/or recreation.

152. As a result of the Data Breach, Plaintiff Gignac anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Gignac will continue to be at increased risk of identity theft and fraud for years to come.

MARYLAND

153. Plaintiff **Joseph I. Frontera** is a resident and citizen of Maryland. Plaintiff Frontera is acting on his own behalf and on behalf of others similarly situated. Defendant obtained and

continues to maintain Plaintiff Frontera's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Frontera would not have entrusted his Private Information to one or more Social Good Entities had he known that one of the entity's primary cloud computing vendors entrusted with his Private Information failed to maintain adequate data security. Plaintiff Frontera's Private Information was compromised and disclosed as a result of the Data Breach.

154. Plaintiff Frontera was required to provide his PHI to his healthcare provider as a predicate to receiving healthcare services. Plaintiff Frontera's PHI was in turn provided to Defendant to be held for safekeeping.

155. In or around September 2020, Plaintiff Frontera received notice from Mercy Health Services that his PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Frontera's PHI, including name, date of birth, certain information relating to health visits to Mercy such as dates and times of those visits, and physicians or departments that provided him with care, was compromised as a result of the Data Breach.

156. This notice further indicated that the Data Breach did not involve the exposure of information such as SSNs or financial card information and/or that certain categories of data were encrypted. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Frontera's was exposed due to Blackbaud's conduct.

157. As a result of the Data Breach, Plaintiff Frontera made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: reviewing credit reports, financial account statements, and/or medical records for any indications of actual or

attempted identity theft or fraud. Plaintiff Frontera now spends approximately one to two hours per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff Frontera has spent at least 30 hours on these tasks, valuable time Plaintiff Frontera otherwise would have spent on other activities, including but not limited to work and/or recreation.

158. Plaintiff Frontera was not offered credit monitoring and identity theft protection services by Blackbaud.

159. As a result of the Data Breach, Plaintiff Frontera has suffered emotional distress as a result of the release of his PHI, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PHI for purposes of identity theft and fraud. Plaintiff Frontera is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

160. Plaintiff Frontera suffered actual injury from having his PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PHI, a form of property that Blackbaud obtained from Plaintiff Frontera; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

161. Moreover, subsequent to the Data Breach, Plaintiff Frontera also experienced actual identity theft and fraud. Plaintiff Frontera has replaced his credit cards twice since the breach as a result of unauthorized credit card purchases at gas stations and mini marts. Credit cards for Neiman Marcus and Helzberg Diamond had been fraudulently opened in his name with charges in excess of \$10,000. In response to these fraudulent charges, Plaintiff Frontera filed a police report. Plaintiff

Frontera was in the process of refinancing his home when an “unpaid” notification showed up on his credit report from the Helzberg Diamond fraudulent charge. Plaintiff Frontera has received scam emails from PayPal and Amazon notifying him that he needs to reset his account or verify information or these accounts will be closed. In addition, Plaintiff Frontera received notification that his Private Information was found on the dark web; has experienced an increased amount of suspicious, unsolicited phishing telephone calls, text messages, and/or emails.

162. Plaintiff Frontera has spent approximately ten hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with this incident resulting from the Data Breach is time Plaintiff Frontera otherwise would have spent on other activities, such as work and/or recreation.

163. As a result of the Data Breach, Plaintiff Frontera anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Frontera will continue to be at increased risk of identity theft and fraud for years to come.

MASSACHUSETTS

164. Based upon counsel’s investigation, and upon information and belief, residents and citizens of the State of Massachusetts were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Massachusetts.

MICHIGAN

165. Based upon counsel’s investigation, and upon information and belief, residents and citizens of the State of Michigan were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Michigan.

MINNESOTA

166. Plaintiff **William Glasper** is a resident and citizen of Minnesota. Plaintiff Glasper is acting on his own behalf and on behalf of others similarly situated. Blackbaud obtained and

continues to maintain Plaintiff Glasper's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Glasper would not have entrusted his Private Information to one or more Social Good Entities had he known that one of the entity's primary cloud computing vendors entrusted with his Private Information failed to maintain adequate data security. Plaintiff Glasper's Private Information was compromised and disclosed as a result of the Data Breach.

167. Plaintiff Glasper was required to provide his PHI to his healthcare provider as a predicate to receiving healthcare services. Plaintiff Glasper's PHI was in turn provided to Blackbaud to be held for safekeeping.

168. In or around September 2020, Plaintiff Glasper received notice from Allina Health that his PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Glasper's PHI, including name and address, date of birth, date of care for patient, name of doctors who admitted or treated Plaintiff Glasper and Allina location visits, was compromised as a result of the Data Breach.

169. This notice further indicated that the Data Breach did not involve the exposure of credit card information, bank account information, SSNs, and any additional medical information, such as diagnosis or treatment plan. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Glasper's was exposed due to Blackbaud's conduct.

170. As a result of the Data Breach, Plaintiff Glasper made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: reviewing financial account statements for any indications of fraud. To date, Plaintiff Glasper has spent at least five

hours dealing with issues related to the Data Breach, valuable time Plaintiff Glasper otherwise would have spent on other activities, including but not limited to work and/or recreation.

171. As a result of the Data Breach, Plaintiff Glasper has suffered emotional distress as a result of the release of his PHI, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PHI for purposes of identity theft and fraud. Plaintiff Glasper is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

172. Plaintiff Glasper was not offered credit monitoring and identity theft protection services by Blackbaud.

173. Plaintiff Glasper suffered actual injury from having his PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PHI, a form of property that Blackbaud obtained from Plaintiff Glasper; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

174. Moreover, subsequent to the Data Breach, Plaintiff Glasper also experienced a significant increase in suspicious, unsolicited phishing telephone calls, text messages, and/or emails. Plaintiff Glasper spent approximately 10 hours dealing with these issues.

175. As a result of the Data Breach, Plaintiff Glasper anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Glasper will continue to be at increased risk of identity theft and fraud for years to come.

176. Plaintiff **Eric Mandel** is a resident and citizen of Minnesota. Plaintiff Mandel is acting on his own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Mandel's Private Information and has a legal duty and obligation

to protect that Private Information from unauthorized access and disclosure. Plaintiff Mandel would not have entrusted his Private Information to one or more Social Good Entities had he known that one of the entity's primary cloud computing vendors entrusted with his Private Information failed to maintain adequate data security. Plaintiff Mandel's Private Information was compromised and disclosed as a result of the Data Breach.

177. Plaintiff Mandel was required to provide his PHI to his healthcare provider as a predicate to receiving healthcare services. Plaintiff Mandel's PHI was in turn provided to Blackbaud to be held for safekeeping.

178. In or around September 2020, Plaintiff Mandel received notice from Allina Health that his PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Mandel's PHI including his name, address, date of birth, dates he was cared for, the names of the doctors who treated him, and the locations he visited, was compromised as a result of the Data Breach.

179. This notice further indicated that the Data Breach did not involve the exposure of credit card information, bank account information, SSNs and any additional medical information, such as diagnosis or treatment plan and/or that certain categories of data were encrypted. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best.

180. As a result of the Data Breach, Plaintiff Mandel made reasonable efforts to mitigate its impact after receiving the notification letter, including reviewing financial account statements, validating charges, and freezing his credit. Plaintiff Mandel now spends approximately two to three hours per month reviewing account statements for irregularities. To date, Plaintiff has spent

at least ten hours on these tasks, valuable time Plaintiff Mandel otherwise would have spent on other activities, including but not limited to work and/or recreation.

181. Plaintiff Mandel was not offered credit monitoring and identity theft protection services by Blackbaud.

182. As a result of the Data Breach, Plaintiff Mandel has suffered emotional distress as a result of the release of his Private Information, including PHI, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff Mandel is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

183. Plaintiff Mandel suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Blackbaud obtained from Plaintiff Mandel; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

184. Moreover, subsequent to the Data Breach, Plaintiff Mandel also experienced actual identity theft and fraud, including a significant increase in suspicious, unsolicited phishing telephone calls, text messages, and/or emails. Plaintiff Mandel has spent at least three hours reviewing these suspicious calls and emails as a result of the Data Breach and will continue to do so. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Mandel otherwise would have spent on other activities, such as work and/or recreation.

185. As a result of the Data Breach, Plaintiff Mandel anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data

Breach. Plaintiff Mandel will continue to be at increased risk of identity theft and fraud for years to come.

MISSISSIPPI

186. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Mississippi were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Mississippi.

MISSOURI

187. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Missouri were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Missouri.

MONTANA

188. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Montana were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of this Montana.

NEBRASKA

189. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Nebraska were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Nebraska.

NEVADA

190. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Nevada were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of this Nevada.

NEW HAMPSHIRE

191. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of New Hampshire were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of New Hampshire.

NEW JERSEY

192. Plaintiff **Donna Steinhorn** is a resident and citizen of New Jersey. Plaintiff Steinhorn is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Steinhorn's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Steinhorn would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Steinhorn's Private Information was compromised and disclosed as a result of the Data Breach.

193. In or around July 2020, Plaintiff Steinhorn received notice from the ACLU that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Steinhorn's PII, including donor information, were compromised as a result of the Data Breach. This notice further indicated that the Data Breach did not involve the exposure of credit card or bank account information. Further, the ACLU noted, "In all candor, we are frustrated with the lack of information we've received from Blackbaud about this incident thus far."

194. In or around August 2020, Plaintiff Steinhorn received notice from the Hunter College High School Alumni Association that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Steinhorn's PII, including names, addresses, giving history, and event participation history, were compromised as

a result of the Data Breach. This notice further indicated that the Data Breach did not involve the exposure of highly sensitive data such as usernames and passwords, and credit card and banking information, because that data had been encrypted.

195. Each of Plaintiff Steinhorn's notices from the ACLU and the Hunter College High School Alumni Association noted that information including financial information was not exposed. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus, at this time, it is unclear how much PII of Plaintiff Steinhorn's was exposed due to Blackbaud's conduct.

196. As a result of the Data Breach, Plaintiff Steinhorn made reasonable efforts to mitigate its impact after receiving the notification emails, including but not limited to: researching the Data Breach and Blackbaud; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud and researching credit monitoring and identity theft protection services. Plaintiff Steinhorn now spends at least two hours per month reviewing her credit card statements and bank account statements for irregularities. This is valuable time Plaintiff Steinhorn otherwise would have spent on other activities, including but not limited to work and/or recreation.

197. Plaintiff Steinhorn was not offered credit monitoring and identity theft protection services by Blackbaud.

198. As a result of the Data Breach, Plaintiff Steinhorn has suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Steinhorn is very concerned about identity

theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

199. Plaintiff Steinhorn suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Blackbaud obtained from Plaintiff Steinhorn; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

200. Moreover, subsequent to the Data Breach, Plaintiff Steinhorn also experienced actual fraud, including an increase in suspicious, unsolicited phishing telephone calls, text messages, and/or emails. In addition, she has received notifications that her personal information has been found on the “dark web.”

201. To date, Plaintiff Steinhorn has spent twelve hours responding to these incidents as a result of the Data Breach. The time spent dealing with this incident resulting from the Data Breach is time Plaintiff Steinhorn otherwise would have spent on other activities, such as work and/or recreation.

202. As a result of the Data Breach, Plaintiff Steinhorn anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Steinhorn will continue to be at increased risk of identity theft and fraud for years to come.

203. Plaintiff **Rachel Roth** is a resident and citizen of New York. Plaintiff Roth is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Roth’s Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Roth would not have entrusted her Private Information to one or more Social Good Entities had she known that one of

the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Roth's Private Information was compromised and disclosed as a result of the Data Breach.

204. In or around August 2020, Plaintiff Roth received notice from the Joseph Kushner Hebrew Academy that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Roth's PII, including her name, address, date of birth and giving history, may have been compromised as a result of the Data Breach with an assurance that the cyber criminals did not gain access to SSNs. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best.

205. On November 23, 2020, Plaintiff Roth received an updated notice from Joseph Kushner Hebrew Academy informing her that certain information, maintained on the legacy software, previously believed to be encrypted, was not encrypted and that the compromised file may have contained Roth's SSN. Plaintiff Roth attended Joseph Kushner Hebrew Academy from approximately 2005 through 2014. Thus, at this time it is unclear how much Private Information of Plaintiff Roth's was exposed due to Blackbaud's conduct.

206. As a result of the Data Breach, Plaintiff tried to mitigate its impact after receiving the notification letters, including researching the Data Breach and Blackbaud; reviewing financial account statements, for any indications of actual or attempted identity theft or fraud. Plaintiff Roth now spends at least 25 minutes per month reviewing her credit card statements and bank account statements checking for irregularities. To date, Plaintiff has spent at least 5 hours on these tasks, valuable time Plaintiff Roth otherwise would have spent on other activities, including but not limited to work and/or recreation.

207. As a result of the Data Breach, Plaintiff Roth has suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Roth is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

208. Plaintiff Roth was offered credit monitoring services from Blackbaud, but would not accept the offer because she does not trust Blackbaud or any service that they are offering.

209. Plaintiff Roth suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Blackbaud obtained from Plaintiff Roth; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

210. Moreover, subsequent to the Data Breach, Plaintiff Roth also experienced actual identity theft and fraud, including an alert on February 11, 2020 from Capital One that her information was found on the dark web.

211. As a result of the Data Breach, Plaintiff Roth anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Roth will continue to be at increased risk of identity theft and fraud for years to come.

NEW MEXICO

212. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of New Mexico were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of New Mexico.

NEW YORK

213. Plaintiff **Ralph Peragine** is a resident and citizen of New York. Plaintiff Peragine is acting on his own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Peragine's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Peragine would not have entrusted his Private Information to one or more Social Good Entities had he known that one of the entity's primary cloud computing vendors entrusted with his Private Information failed to maintain adequate data security. Plaintiff Peragine's Private Information was compromised and disclosed as a result of the Data Breach.

214. Plaintiff Peragine was required to provide his PHI to his healthcare provider as a predicate to receiving healthcare services. Plaintiff Peragine's PHI was in turn provided to Blackbaud to be held for safekeeping.

215. In or around October 2020, Plaintiff Peragine received notice from New Haven Hospital that his PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Peragine's PHI, including name, address, phone number, date of birth, philanthropic history, name of doctor and dates of service at the hospital, was compromised as a result of the Data Breach.

216. This notice further indicated that the Data Breach did not involve the exposure of bank accounts, credit cards, SSNs, and/or that certain categories of data were encrypted. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus, at this time, it is unclear how much PII of Plaintiff Peragine's was exposed due to Blackbaud's conduct.

217. As a result of the Data Breach, Plaintiff Peragine made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: reviewing

credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud. Plaintiff Peragine now spends approximately 30 minutes per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least three hours on these tasks, valuable time Plaintiff Peragine otherwise would have spent on other activities, including but not limited to work and/or recreation.

218. Plaintiff Peragine was not offered credit monitoring and identity theft protection services by Blackbaud.

219. As a result of the Data Breach, Plaintiff Peragine has suffered emotional distress as a result of the release of his Private Information, including PHI, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Peragine is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

220. Plaintiff Peragine suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Blackbaud obtained from Plaintiff Peragine; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

221. Moreover, subsequent to the Data Breach, Plaintiff Peragine also experienced actual identity theft and fraud. Someone applied for and received unemployment benefits in Plaintiff Peragine's name. Plaintiff Peragine filed a notice on the New York Department of Labor website indicating that he had not applied for unemployment benefits. Plaintiff Peragine spent approximately one hour responding to this incident of identity theft and fraud as a result of the

Data Breach. The time spent dealing with this incident resulting from the Data Breach is time Plaintiff Peragine otherwise would have spent on other activities, such as work and/or recreation.

222. As a result of the Data Breach, Plaintiff Peragine anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Peragine will continue to be at increased risk of identity theft and fraud for years to come.

223. Plaintiff **Karen Zielinski** is a resident and citizen of New York. Plaintiff Zielinski is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Zielinski's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Zielinski would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Zielinski's Private Information was compromised and disclosed as a result of the Data Breach.

224. Plaintiff Zielinski was required to provide her PII to entities to whom she regularly made charitable donations. Plaintiff Zielinski's PII was in turn provided to Blackbaud to be held for safekeeping. In or around September 2020, Plaintiff Zielinski received notice from the Roswell Park Alliance Foundation that her PII had been improperly accessed and/or obtained by unauthorized third parties and notice from the Light of Life Rescue Mission informing her about the Blackbaud Data Breach.

225. The Roswell Park Alliance Foundation notice indicated that Plaintiff Zielinski's PII, including non-financial information, contact information, date of birth, limited demographic data and a history of her relationship with the Alliance Foundation such as donation dates and amounts, was compromised as a result of the Data Breach.

226. The Rosewell Park Alliance Foundation notice further indicated that the Data Breach did not involve the exposure of usernames, passwords, credit card information, bank account information, SSNs and/or that certain categories of data were encrypted. The Light of Life Rescue Mission notice indicated that the Data Breach did not involve usernames, passwords, credit card information, bank account information, or SSNs. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus, at this time, it is unclear how much Private Information of Plaintiff Zielinski's was exposed due to Blackbaud's conduct.

227. As a result of the Data Breach, Plaintiff Zielinski made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: researching the Data Breach and Blackbaud; reviewing credit reports, financial account statements for any indications of actual or attempted identity theft or fraud; and unsubscribing from scam emails. Plaintiff Zielinski has spent approximately 20 hours per month reviewing credit monitoring reports and/or checking account statements for irregularities and continues to do so. This is valuable time Plaintiff Zielinski otherwise would have spent on other activities, including but not limited to work and/or recreation.

228. Plaintiff Zielinski was not offered credit monitoring and identity theft protection services by Blackbaud.

229. As a result of the Data Breach, Plaintiff Zielinski has suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Zielinski is very concerned about identity theft

and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

230. Plaintiff Zielinski suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Blackbaud obtained from Plaintiff Zielinski; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

231. Moreover, subsequent to the Data Breach, Plaintiff Zielinski also experienced actual identity theft and fraud, including a significant increase in the amount of suspicious, unsolicited phishing telephone calls, text messages, and/or emails. Plaintiff Zielinski spends a tremendous amount of time dealing with multiple scam phone calls every day and unsubscribing to scam emails. Plaintiff Zielinski spent approximately 30 hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Zielinski otherwise would have spent on other activities, such as work and/or recreation.

232. As a result of the Data Breach, Plaintiff Zielinski anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Zielinski will continue to be at increased risk of identity theft and fraud for years to come.

NORTH CAROLINA

233. Plaintiff **William Allen** is a resident and citizen of North Carolina. Plaintiff Allen is acting on his own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Allen's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Allen would not have entrusted his Private Information to one or more Social Good Entities had he known that

one of the entity's primary cloud computing vendors entrusted with his Private Information failed to maintain adequate data security. Plaintiff Allen's Private Information was compromised and disclosed as a result of the Data Breach.

234. In or around August 2020, Plaintiff Allen received notices from WakeMed Foundation and Episcopal High School that his PII had been improperly accessed and/or obtained by unauthorized third parties. The WakeMed Foundation notice indicated that Plaintiff Allen's PII, including name, title, date of birth, spouse, phone numbers and email addresses were compromised as a result of the Data Breach. The Episcopal High School notice indicated that Plaintiff Allen's PII, including names, dates of birth, address/contact information, relationships, and giving history.

235. The WakeMed notice further indicated that the Data Breach did not involve encrypted information, such as SSNs, bank account, or credit/debit card information. The Episcopal High School notice further indicated that the Data Breach did not involve credit card information, bank account data, or other sensitive information. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Allen's was exposed due to Blackbaud's conduct.

236. As a result of the Data Breach, Plaintiff Allen made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: purchasing or continuing to maintain credit monitoring services; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Allen now spends approximately 10 to 15 hours per month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least 30 hours on these

tasks, valuable time Plaintiff Allen otherwise would have spent on other activities, including but not limited to work and/or recreation.

237. Since Plaintiff Allen was not offered credit monitoring and identity theft protection services by Blackbaud, Plaintiff Allen has purchased credit monitoring and identity theft protection services on an annual basis for approximately \$99.99 per year. Plaintiff Allen plans to continue purchasing credit monitoring and identity theft protection services on an ongoing basis to protect himself from identity theft and fraud.

238. As a result of the Data Breach, Plaintiff Allen has suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Allen is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

239. Plaintiff Allen suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Blackbaud obtained from Plaintiff Allen; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

240. Moreover, subsequent to the Data Breach, Plaintiff Allen also experienced a significant increase in suspicious, unsolicited phishing telephone calls, text messages, and/or emails. Plaintiff Allen has spent several hours dealing with these issues.

241. As a result of the Data Breach, Plaintiff Allen anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Allen will continue to be at increased risk of identity theft and fraud for years to come.

242. Plaintiff **Coty Martin** is a resident and citizen of North Carolina. Plaintiff Martin is acting on his own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Martin's and his minor child's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Martin would not have entrusted his or his minor child's Private Information to one or more Social Good Entities had he known that one of the entity's primary cloud computing vendors entrusted with his and his minor child's Private Information failed to maintain adequate data security. Plaintiff Martin's and his minor child's Private Information was compromised and disclosed as a result of the Data Breach.

243. Plaintiff Martin was required to provide his minor son's PHI to his healthcare provider as a predicate to receiving healthcare services. Plaintiff Martin's minor son's PHI and Plaintiff Martin's PII was in turn provided to Defendant to be held for safekeeping.

244. In or around August 2020, Plaintiff Martin received notice from Atrium Health that his minor child's PHI and his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Martin's PII and his minor child's PHI, including his minor child's first and last name and contact information (such as home address, phone number and email), certain demographic information (including date of birth, guarantor information, and internally generated patient ID numbers), the dates of treatment, the locations of service, and the name of the treating physician and may also have included the name and relationship of his child's guarantor, such as a parent or guardian, and donor information, was compromised as a result of the Data Breach.

245. This notice further indicated that the Data Breach did not involve the exposure of SSNs, credit card information or bank account information. The notice further states that

Blackbaud does not have access to Plaintiff Martin's minor child's medical record nor any information about his minor child's prognosis, medications, or test results. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Martin's and his minor child's was exposed due to Blackbaud's conduct.

246. As a result of the Data Breach, Plaintiff Martin made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: purchasing credit monitoring services; reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud. Plaintiff Martin now spends at least an hour each week or every other week reviewing credit card and bank account statements for irregularities and has spent many hours dealing with issues related to the Data Breach. This is valuable time Plaintiff Martin otherwise would have spent on other activities, including but not limited to work and/or recreation.

247. Since Plaintiff Martin was not offered credit monitoring and identity theft protection services by Blackbaud, Plaintiff Martin has purchased credit monitoring and identity theft protection services on a monthly basis for approximately \$12.90 per month. Plaintiff Martin plans to continue purchasing credit monitoring and identity theft protection services on an ongoing basis to protect him and his family from identity theft and fraud.

248. As a result of the Data Breach, Plaintiff Martin has suffered emotional distress as a result of the release of his PII and his minor son's PHI, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII and his minor son's PHI for purposes of identity theft and fraud. Plaintiff

Martin is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

249. Plaintiff Martin and his minor son have suffered actual injury from having his PII and his minor son's PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII and his minor son's PHI, a form of property that Blackbaud obtained from Plaintiff Martin; (b) violation of his and his minor son's privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

250. Moreover, subsequent to the Data Breach, Plaintiff Martin also experienced actual identity theft and fraud including notification that his Private Information was found on the dark web and receives suspicious, unsolicited phishing telephone calls on a daily basis.

251. As a result of the Data Breach, Plaintiff Martin anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Martin will continue to be at increased risk of identity theft and fraud for years to come.

NORTH DAKOTA

252. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of North Dakota were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of North Dakota.

OHIO

253. Plaintiff **Michele Pettiford** is a resident and citizen of Ohio. Plaintiff Pettiford is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Pettiford's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Pettiford would not have entrusted her Private Information to one or more Social Good Entities had her

known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Pettiford's Private Information was compromised and disclosed as a result of the Data Breach.

254. In or around September 2020, Plaintiff Pettiford received notice from the Smithsonian Institution that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Pettiford's PII including demographic information such as names, U.S. addresses, phone numbers, and summary of donations, was compromised as a result of the Data Breach.

255. This notice further indicated that the Data Breach did not involve the exposure of any credit card information, SSNs, banking information or other similar data. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus, at this time, it is unclear how much PII of Plaintiff Pettiford's was exposed due to Blackbaud's conduct.

256. As a result of the Data Breach, Plaintiff Pettiford made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: purchasing or maintaining credit monitoring services; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Pettiford now spends approximately ten hours per month reviewing credit monitoring reports and/or checking account statements for irregularities since the data breach to present. This is valuable time Plaintiff Pettiford otherwise would have spent on other activities, including but not limited to work and/or recreation.

257. Since Plaintiff Pettiford was not offered credit monitoring and identity theft protection services by Blackbaud, Plaintiff Pettiford has elected to maintain credit monitoring and

identity theft protection services on a monthly basis for approximately \$24.95 per month. Plaintiff Pettiford plans to continue purchasing credit monitoring and identity theft protection services on an ongoing basis to protect herself from identity theft and fraud.

258. As a result of the Data Breach, Plaintiff Pettiford has suffered emotional distress resulting from the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Pettiford is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

259. Plaintiff Pettiford suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Blackbaud obtained from Plaintiff Pettiford; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

260. Moreover, subsequent to the Data Breach, Plaintiff Pettiford also experienced actual identity theft and fraud. An unknown individual fraudulently applied for unemployment benefits in her name and received \$14,280. In order to fix the issue, Plaintiff Pettiford had to call the unemployment office where she was instructed to file a fraud charge on the government website. In addition, Plaintiff Pettiford had two unauthorized attempted charges on her American Express card and has received notifications that her PII information was found on the dark web. Plaintiff Pettiford has also experienced a significant increase in suspicious, unsolicited phishing telephone calls, text messages, and/or emails.

261. Plaintiff Pettiford has spent approximately 80 hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Pettiford otherwise would have spent on other activities, such as work and/or recreation.

262. As a result of the Data Breach, Plaintiff Pettiford anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Pettiford will continue to be at increased risk of identity theft and fraud for years to come.

OKLAHOMA

263. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Oklahoma were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Oklahoma.

OREGON

264. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Oregon were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Oregon.

PENNSYLVANIA

265. Plaintiff **Christina Duranko** is a resident and citizen of Pennsylvania. Plaintiff Duranko is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Duranko's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Duranko would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private

Information failed to maintain adequate data security. Plaintiff Duranko's Private Information was compromised and disclosed as a result of the Data Breach.

266. Plaintiff Duranko was required to provide her PHI to her healthcare provider as a predicate to receiving healthcare services. Plaintiff Duranko's PHI was in turn provided to Blackbaud to be held for safekeeping.

267. In or around December 4, 2020, Plaintiff Duranko received notice from Allegheny Health Network ("AHN") that her PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Duranko's PHI, including name, date of birth, address, business address, phone numbers, email addresses, and limited medical information, such as dates she may have had services provided at AHN, her treating provider's name, and the AHN location, may have been compromised as a result of the Data Breach.

268. This notice further indicated that the Data Breach did not involve the exposure of credit card information, bank account information, or SSNs. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus, at this time, it is unclear how much Private Information of Plaintiff Duranko's was exposed due to Blackbaud's conduct.

269. As a result of the Data Breach, Plaintiff Duranko made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: researching the Data Breach and Blackbaud; reviewing credit reports and financial account statements and/or medical records for any indications of actual or attempted identity theft or fraud, including placing a credit freeze on her Equifax credit report. In addition, as a result of the Data Breach, Plaintiff Duranko vigorously confirms each of her medical provider's treatment recommendations to make sure that they are based on accurate medical history. Plaintiff Duranko has also sent

correspondence to AHN's Chief Privacy Officer concerning the disclosure and distribution of her PHI in order to request an accounting of the information that was stolen. Plaintiff Duranko now spends at least one hour per month reviewing credit monitoring reports and/or checking account statements and additional time reviewing her medical records as she receives them for irregularities. To date, Plaintiff has spent at least 10 hours on these tasks, valuable time Plaintiff Duranko otherwise would have spent on other activities, including but not limited to work and/or recreation.

270. Plaintiff Duranko was not offered credit monitoring and identity theft protection services by Blackbaud.

271. As a result of the Data Breach, Plaintiff Duranko has suffered emotional distress as a result of the release of her PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PHI for purposes of identity theft and fraud. Plaintiff Duranko is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

272. Plaintiff Duranko suffered actual injury from having her PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PHI, a form of property that Blackbaud obtained from Plaintiff Duranko; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

273. As a result of the Data Breach, Plaintiff Duranko anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data

Breach. Plaintiff Duranko will continue to be at increased risk of identity theft and fraud for years to come.

PUERTO RICO

274. Based upon counsel's investigation, and upon information and belief, residents and citizens of Puerto Rico were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Puerto Rico.

RHODE ISLAND

275. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Rhode Island were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Rhode Island.

SOUTH CAROLINA

276. Plaintiff **Latricia Ford** is a resident and citizen of South Carolina. Plaintiff Ford is acting on her own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Ford's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Ford would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Ford's Private Information was compromised and disclosed as a result of the Data Breach.

277. Plaintiff Ford was required to provide her PHI to her healthcare provider as a predicate to receiving healthcare services. Plaintiff Ford's PHI was in turn provided to Defendant to be held for safekeeping.

278. In or around September 2020, Plaintiff Ford received notice from Roper St. Francis Healthcare that her PHI had been improperly accessed and/or obtained by unauthorized third

parties. This notice indicated that Plaintiff Ford's PHI, including name, gender, date of birth, address, date(s) of treatment, department(s) of service, and treating physician(s) were compromised as a result of the Data Breach.

279. This notice further indicated that the Data Breach did not involve the exposure of SSNs, financial account information, credit card information, or electronic health records. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus, at this time, it is unclear how much PHI of Plaintiff Ford's was exposed due to Blackbaud's conduct.

280. As a result of the Data Breach, Plaintiff Ford made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: reviewing explanation of benefit statements from health care providers for which Plaintiff Ford spends approximately one hour per month reviewing these statements for irregularities. To date, Plaintiff Ford has spent at least six hours on these tasks, valuable time Plaintiff Ford otherwise would have spent on other activities, including but not limited to work and/or recreation.

281. Plaintiff Ford was not offered credit monitoring and identity theft protection services by Blackbaud.

282. As a result of the Data Breach, Plaintiff Ford has suffered emotional distress as a result of the release of her PHI, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PHI for purposes of identity theft and fraud. Plaintiff Ford is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

283. Plaintiff Ford suffered actual injury from having her PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her

PHI, a form of property that Blackbaud obtained from Plaintiff Ford; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

284. Moreover, subsequent to the Data Breach, Plaintiff Ford also experienced actual fraud and identity theft, including an increase in suspicious emails and phone calls. Plaintiff Ford has received numerous cyber alerts from MyIDCare where she was informed that individuals had gained knowledge of her name, email, previous home address and telephone number. Plaintiff Ford received a fraudulent phone call from someone impersonating her internet provider who attempted to gain access to her work computer; and has also been notified that someone had requested an insurance quote in her name from State Farm Insurance for a vehicle Plaintiff Ford does not own and in connection with this request for an insurance quote, State Farm did a soft inquiry on her credit.

285. Plaintiff Ford spent approximately four hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Ford otherwise would have spent on other activities, such as work and/or recreation.

286. As a result of the Data Breach, Plaintiff Ford anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Ford will continue to be at increased risk of identity theft and fraud for years to come.

287. Plaintiff **Clifford Scott** is a resident and citizen of South Carolina. Plaintiff Scott is acting on his own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Scott's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Scott would not

have entrusted his Private Information to one or more Social Good Entities had he known that one of the entity's primary cloud computing vendors entrusted with him Private Information failed to maintain adequate data security. Plaintiff Scott's Private Information was compromised and disclosed as a result of the Data Breach.

288. Plaintiff Scott was required to provide his PII to entities to whom he made charitable donations. Plaintiff Scott's PII was in turn provided to Defendant to be held for safekeeping.

289. In or around September 2020, Plaintiff Scott received notice from the University of South Carolina that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Scott's PII, including name, contact information, demographic information, date of birth and giving profiles and history were compromised as a result of the Data Breach.

290. As a result of the Data Breach, Plaintiff Scott made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: reviewing financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Scott spends at least 2 hours per month reviewing these statements for irregularities. This is valuable time Plaintiff Scott otherwise would have spent on other activities, including but not limited to work and/or recreation.

291. Plaintiff Scott was not offered credit monitoring and identity theft protection services by Blackbaud.

292. As a result of the Data Breach, Plaintiff Scott has suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII

for purposes of identity theft and fraud. Plaintiff Scott is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach

293. Plaintiff Scott suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Blackbaud obtained from Plaintiff Scott; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

294. Moreover, subsequent to the Data Breach, Plaintiff Scott also experienced actual fraud, including an increase in suspicious text messages and phone calls. In addition, Plaintiff Scott's email and phone number have been found on the dark web. Plaintiff Scott has spent numerous hours responding to these incidents of identity theft and fraud as a result of the Data Breach and dealing with the Data Breach in general. The time spent dealing with this incident resulting from the Data Breach is time Plaintiff Scott otherwise would have spent on other activities, such as work and/or recreation.

295. As a result of the Data Breach, Plaintiff Scott anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Scott will continue to be at increased risk of identity theft and fraud for years to come.

SOUTH DAKOTA

296. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of South Dakota were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of South Dakota.

TENNESSEE

297. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Tennessee were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Tennessee.

TEXAS

298. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Texas were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Texas.

UTAH

299. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Utah were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Utah.

VERMONT

300. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Vermont were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Vermont.

VIRGIN ISLANDS

301. Based upon counsel's investigation, and upon information and belief, residents and citizens of the Virgin Islands were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of the Virgin Islands.

VIRGINIA

302. Based upon counsel's investigation, and upon information and belief, residents and citizens of the Commonwealth of Virginia were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Virginia.

WASHINGTON

303. Plaintiff **Jessica Case** is a resident and citizen of Washington. Plaintiff Case is acting on her own behalf and on behalf of others similarly situated. Blackbaud obtained and continues to maintain Plaintiff Case's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Case would not have entrusted her Private Information to one or more Social Good Entities had she known that one of the entity's primary cloud computing vendors entrusted with her Private Information failed to maintain adequate data security. Plaintiff Case's Private Information was compromised and disclosed as a result of the Data Breach.

304. Plaintiff Case was required to provide her PII to multiple entities as a donor to their organizations. Plaintiff Case's PII was in turn provided to Blackbaud to be held for safekeeping.

305. The first notice Plaintiff Case received with regard to the improper access of her Private Information was in or around July 2020, when she received notice from the Northwest Immigrants Rights Project that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. This indicated that Plaintiff Case's Private Information, including her name, contact information from August 2019, including telephone numbers, email addresses, and mailing addresses, and a history of her relationship with the organization up to that point, such as donation dates and amounts, was compromised as a result of the Data Breach.

306. Plaintiff Case later received notices from the following entities that her Private Information was breached: the Hispanic Federation (certain PII exposed); Shoreline Community College Foundation (certain PII exposed); Wing Luke Museum (certain PII exposed); Planned Parenthood of Great Northwest and the Hawaiian Islands (certain PII exposed); Pomona College (certain PII exposed); International Refugee Assistance Project (certain PII exposed, noting "In

full transparency, we have been dissatisfied with the level of information provided by Blackbaud following this breach as the privacy and confidentiality of our supporters and the individuals we serve are of the utmost importance to IRAP.”); ACLU (certain PII exposed, noting “In all candor, we are frustrated with the lack of information we've received from Blackbaud about this incident thus far.”); Florence Immigrant and Refugee Rights Project (certain PII exposed); P.A.W.S. (Pets Are Worth Saving) (certain PII exposed).

307. While many of these notices indicated that the Data Breach did not involve the exposure of credit card information, bank account information, SSNs or additional medical information, such as diagnosis or treatment plan and/or that certain categories of data were encrypted, later forensic investigations have revealed that Blackbaud’s representations about what information was exposed and/or encrypted were inaccurate at best. Thus at this time, it is unclear how much Private Information of Plaintiff Case’s was exposed due to Blackbaud’s conduct.

308. As a result of the Data Breach, Plaintiff Case made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to, maintaining credit monitoring. Since Plaintiff Case was not offered credit monitoring and identity theft protection services by Blackbaud, Plaintiff Case has purchased, and will continue to purchase, credit monitoring and identity theft protection services from TurboTax Max on an annual basis for approximately \$50 per year. Plaintiff Case plans to continue purchasing credit monitoring and identity theft protection services on an ongoing basis to protect herself from identity theft and fraud.

309. Additionally, Plaintiff Case has spent 5 to 10 hours researching the Data Breach and Blackbaud, resetting passwords to her accounts, looking into changing her phone number, reviewing credit reports, financial account statements, and/or medical records for any indications

of actual or attempted identity theft or fraud. Plaintiff Case now spends significant time each month reviewing credit monitoring reports and/or checking account statements for irregularities. To date, Plaintiff has spent at least 20 to 25 hours on these tasks, valuable time Plaintiff Case otherwise would have spent on other activities, including but not limited to work and/or recreation.

310. As a result of the Data Breach, Plaintiff Case has suffered emotional distress as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff Case is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

311. Plaintiff Case suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Blackbaud obtained from Plaintiff Case; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

312. Moreover, subsequent to the Data Breach, Plaintiff Case also experienced actual identity theft and fraud, including a significantly increased amount of suspicious, unsolicited phishing telephone calls, text messages, and/or emails, as well as notice that her phone number had been compromised by her credit monitoring service provider.

313. Plaintiff Case has spent approximately 20 to 25 hours responding to these incidents of identity theft and fraud as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Case otherwise would have spent on other activities, such as work and/or recreation.

314. As a result of the Data Breach, Plaintiff Case anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Case will continue to be at increased risk of identity theft and fraud for years to come.

315. Plaintiff **Abhi Sheth** is a resident and citizen of Washington. Plaintiff Sheth is acting on his own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Sheth's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Sheth would not have entrusted his Private Information to one or more Social Good Entities had he known that one of the entity's primary cloud computing vendors entrusted with his Private Information failed to maintain adequate data security. Plaintiff Sheth's Private Information was compromised and disclosed as a result of the Data Breach.

316. Plaintiff Sheth was required to provide his PII to entities to whom he regularly pays membership fees as well as his PHI to his healthcare provider as a predicate to receiving healthcare services. Plaintiff Sheth's PII and PHI was in turn provided to Defendant to be held for safekeeping.

317. In or around August 2020, Plaintiff Sheth received notice from KidsQuest Children's Museum that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Sheth's PII, including name, birth date, contact information, including telephone numbers, emails and mailing addresses were compromised as a result of the Data Breach. This notice further indicated that the Data Breach did not involve the exposure of donor credit card information, because it had been encrypted.

318. In or around September 2020, Plaintiff Sheth received notice from YMCA Greater Seattle that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Sheth's PII, including contact information, demographic information, and a history of Plaintiff Sheth's relationship with the organization such as donation dates and amounts were compromised as a result of the Data Breach. This notice further indicated that the Data Breach did not involve the exposure of SSNs, financial account information and/or payment card information, as they were encrypted except there may be exceptions for those who paid by check.

319. In or around September 2020, Plaintiff Sheth received notice from the Virginia Mason Medical Center that his PHI had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Sheth's PHI, including name, contact information—specifically email address and telephone number, gender, date of birth, visit date and location, treating physician(s), and/or concierge medicine status. This notice further indicated that the Data Breach did not involve the exposure of SSNs, bank account and credit card account information because they were encrypted.

320. Each of Plaintiff Sheth's notices from each entity noted that information including SSNs and other financial information was not exposed. However, later forensic investigations have revealed that Blackbaud's representations about what information was exposed and/or encrypted, including SSNs, were inaccurate at best. Thus, at this time, it is unclear how much PII and PHI of Plaintiff Sheth's was exposed due to Blackbaud's conduct.

321. As a result of the Data Breach, Plaintiff Sheth made reasonable efforts to mitigate its impact after receiving the notification letter, including but not limited to: researching the Data Breach; reviewing financial account statements, and/or medical records for any indications of

actual or attempted identity theft or fraud. Plaintiff Sheth has spent approximately 10 hours to date reviewing his credit card and bank statements for irregularities. This is valuable time Plaintiff Sheth otherwise would have spent on other activities, including but not limited to work and/or recreation.

322. Plaintiff Sheth was not offered credit monitoring and identity theft protection services by Blackbaud.

323. As a result of the Data Breach, Plaintiff Sheth has suffered emotional distress as a result of the release of his PII and PHI, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII and PHI for purposes of identity theft and fraud. Plaintiff Sheth is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

324. Plaintiff Sheth suffered actual injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII and PHI, a form of property that Blackbaud obtained from Plaintiff Sheth; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

325. Moreover, subsequent to the Data Breach, Plaintiff Sheth also experienced actual fraud, including an increase in suspicious emails and phone calls and he has received notification that his login credentials were found on the dark web. In response to this, Plaintiff Sheth had to change his password on many of his accounts.

326. Plaintiff Sheth has spent 50 hours dealing with the results of the Data Breach. The time spent dealing with this incident resulting from the Data Breach is time Plaintiff Sheth otherwise would have spent on other activities, such as work and/or recreation.

327. As a result of the Data Breach, Plaintiff Sheth anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Sheth will continue to be at increased risk of identity theft and fraud for years to come.

WEST VIRGINIA

328. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of West Virginia were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of West Virginia.

WISCONSIN

329. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Wisconsin were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Wisconsin.

WYOMING

330. Based upon counsel's investigation, and upon information and belief, residents and citizens of the State of Wyoming were impacted by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of Wyoming.

B. Defendant

331. Defendant Blackbaud, Inc. is a Delaware corporation with its principal place of business located at 65 Fairchild Street, Charleston, South Carolina. Blackbaud's common stock is publicly traded on the NASDAQ under the ticker symbol "BLKB." Blackbaud manages, maintains, and provides cloud computing software, services, and cybersecurity for clients

including healthcare organizations, education institutions, and other non-profit corporations,⁵¹ including the non-profits which obtained and maintained Plaintiffs' Private Information that was compromised in the Data Breach. Blackbaud has "over 45,000 customers located in over 100 countries."⁵²

IV. JURISDICTION AND VENUE

332. This Consolidated Complaint is intended to serve as a superseding complaint as to all other complaints consolidated in this multidistrict litigation and other complaints filed in this District and transferred to the same Court overseeing the multidistrict litigation, and to serve for all purposes as the operative pleading. To the extent additional causes of action are presented against additional defendants, Plaintiffs reserve the right to propose case management procedures to ensure the efficient and effective litigation of this multidistrict litigation, or to seek leave to amend the operative complaint.

333. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1711, *et seq.*, because at least one member of the Class, as defined below, is a citizen of a different state than Blackbaud, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds \$5,000,000, exclusive of interest and costs.

334. This Court has personal jurisdiction over this action because Blackbaud maintains its principal place of business in this District, has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District, such that it

⁵¹ See *About Blackbaud*, Blackbaud, <https://www.blackbaud.com/company> (last visited Mar. 15, 2021) [<https://perma.cc/Z5FL-6A9L>].

⁵² 2019 Form 10-K, *supra* n.21.

could reasonably foresee litigation being brought in this District. This Court also has diversity jurisdiction over this action. *See* 28 U.S.C. § 1332(a).

335. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Blackbaud's principal place of business is located in this District and a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District. Venue is also proper in this District pursuant to 28 U.S.C. § 1391(b) based on the transfer order of the Judicial Panel on Multidistrict Litigation.

V. **STATEMENT OF FACTS**

A. **A Sophisticated Cloud-Service Provider, Blackbaud Knew of the Risk That Cybercriminals Posed to Hosted Data**

336. Incorporated in 1982, Blackbaud describes itself as "the world's leading cloud software company powering social good."⁵³ It provides "cloud software, services, expertise and data intelligence," which its clients use for administration, fundraising, and financial management.⁵⁴

337. Blackbaud is a publicly-traded company with clients that include "nonprofits, foundations, corporations, education institutions, healthcare institutions, and the individual change agents who support them."⁵⁵ Blackbaud specifically markets its products to these entities, noting the robust data security policies and protections it has in place to safeguard the Private Information of donors, students, congregants, and patients. The Social Good Entities process sensitive information about individuals' financial status, health, and/or educational background in order to perform their missions and raise money.

⁵³ 2019 Form 10-K, *supra* n.21.

⁵⁴ *Id.*

⁵⁵ *Supra* n.51.

338. This marketing has proved to be a lucrative business for Blackbaud, which reported that, “[a]t the end of 2019, [it] had over 45,000 customers located in over 100 countries[,]” with a “total addressable market (“TAM”) . . . greater than \$10 billion.”⁵⁶ Blackbaud’s business depends upon the need to process and keep safe the Private Information of millions of individuals every day.

339. In the ordinary course of doing business with Blackbaud’s clients, individuals are regularly required to provide Private Information that is collected, stored, maintained, and secured by Blackbaud. This Private Information includes one or several of the following categories of data:

- Name;
- Address;
- Phone number(s);
- Email address;
- Date of birth;
- Demographic information;
- SSN;
- Credit card account numbers;
- Bank account numbers;
- Educational history;
- Healthcare records or other data protected under HIPAA;
- Insurance coverage information;
- Photo identification;
- Employer information;
- Income information;
- Donor contribution information; and
- Other Private Information, including passwords, places of birth, and mothers’ maiden names.

⁵⁶ 2019 Form 10-K, *supra* n.21, at 3.

340. This information is valuable and requires someone to provide security; without this Private Information, there is no Blackbaud.

341. Blackbaud collects and stores Private Information from individuals, for which Blackbaud is paid. Blackbaud derives a “significant portion” of its revenue from “transaction-based payment processing fees” that it collects from its customers through the Blackbaud Merchant Services solution, which enables Blackbaud’s customers’ donors to make donations and purchase goods and services using various payment options.⁵⁷ Indeed, based upon the undersigned’s investigation, the more Private Information is housed on its servers, the more Blackbaud charges. In offering and marketing its products, Blackbaud solicits and obtains Private Information of Plaintiffs and Class members from the Social Good Entities for storage on its servers and data analysis. In so doing, Blackbaud offers dedicated services to Social Good Entities, and a significant component and selling point of these services is data security to protect this high-value Private Information.

342. Blackbaud offers a number of solutions and services to power what it purports to be “the world’s most robust philanthropic data set.”⁵⁸ The solutions offered by Blackbaud include fundraising and relationship management, marketing and engagement, financial management, grant and award management, organizational and program management, social responsibility, payment services, and analytics.⁵⁹ The Blackbaud portfolio is “delivered primarily through cloud solutions.”⁶⁰

⁵⁷ 2020 Form 10-K, *supra* n.21, at 18.

⁵⁸ *Id.* at 7.

⁵⁹ *Id.* at 7-10.

⁶⁰ *Id.*

343. The specific solutions offered by Blackbaud are named Blackbaud's Raiser's Edge NXT®; Blackbaud CRM™; Blackbaud eTapestry®; Blackbaud TeamRaiser®; Blackbaud Peer-to-Peer Fundraising™, powered by JustGiving™; Blackbaud Guided Fundraising™ and Blackbaud Volunteer Network Fundraising™; Blackbaud Luminate Online®; Blackbaud Online Express™; Blackbaud School Website System™; Blackbaud Financial Edge NXT®; Blackbaud Tuition Management™; Blackbaud Financial Aid Management™; Blackbaud Grantmaking™; Blackbaud Award Management™; Blackbaud Student Information System™; Blackbaud Learning Management System™; Blackbaud Enrollment Management System™; Blackbaud Altru®; Blackbaud Church Management™; YourCause® Grants Connect® and YourCause CSR Connect®; Blackbaud Merchant Services™; Blackbaud Purchase Cards; and Blackbaud Intelligence for Good®.⁶¹

344. Two of Blackbaud's most popular products include "Blackbaud Raiser's Edge NXT" and "Blackbaud Financial Edge NXT."⁶² With Blackbaud Financial Edge NXT®, Blackbaud uses "advanced technology with powerful reporting tools to help accounting teams drive transparency, stewardship, and compliance while enabling them to seamlessly manage transactions and eliminate manual processes." It also integrates with Blackbaud's Raiser's Edge NXT to "simply gift entry processing and relates information from both systems in an informative manner to eliminate redundant tasks and manual processes."⁶³

345. Blackbaud determines the purposes or means of processing customers' data based on which solutions or services are utilized by the customers. Blackbaud has specific means by

⁶¹ *Id.*

⁶² *Id.* at 7, 8.

⁶³ 2020 Form 10-K, *supra* n.21, at 8.

which it processes payments using Blackbaud Raiser's Edge NXT®, Blackbaud Tuition Management™, Blackbaud Merchant Services™, Blackbaud Purchase Cards, and other tools. Blackbaud describes its payment services as providing its customers "payment processing capabilities that enable their donors to make donations and purchase goods and services using numerous payment options, including credit card and automated clearing house ("ACH") checking transactions, through secure online transactions."⁶⁴

346. It also has specific means by which it processes gifts using Blackbaud eTapestry®, Blackbaud Luminate Online®, and Blackbaud Financial Edge NXT®.⁶⁵

347. Blackbaud also has a specific "intuitive and streamlined application process" it uses for purposes of Blackbaud Award Management™ and a simplified system of sharing student data and academic records securely that it uses in its Blackbaud Student Information System™.⁶⁶

348. In addition to these services, Blackbaud has professional and managed services in which its expert consultants provide data conversion, implementation, and customization services for each of its software solutions, including system implementation; data conversion, business process analysis and application customization; database merging and enrichment, and secure credit card transaction processing; database production activities; and website design services.⁶⁷ In addition, Blackbaud provides consulting services to advise customers on how to improve a business process.⁶⁸

⁶⁴ *Id.* at 9.

⁶⁵ *Id.* at 7-10.

⁶⁶ *Id.* at 8.

⁶⁷ *Id.* at 10-11.

⁶⁸ *Id.* at 10.

349. Blackbaud also touts its Customer Success organization, which “develops and fosters relationships within all levels of the customer organization to build more demonstrated value in [Blackbaud’s] solutions and services, while helping customers achieve their desired outcomes.”⁶⁹ Blackbaud has Customer Success Managers that work with customers to collect and analyze actionable information through direct customer relationships or aggregated analytics that drives future one-to-one or one-to-many interactions. The goal of the Customer Success organization is to “partner with customers to ensure that they are full engaged and have an advocate at Blackbaud who works with them to meet their needs.”⁷⁰

350. In addition to its Customer Success organization, Blackbaud offers customer support and maintenance, which includes up-to-date regular communications, around-the-clock support resources, and Blackbaud’s extensive knowledgebase and forums. Blackbaud also claims to apply its “industry knowledge and experience, combined with expert knowledge of [its] solutions, to evaluate an organization’s needs and consult on how to improve a business process.”⁷¹

B. Blackbaud’s Cybersecurity at the Time of the February 2020

351. Despite Blackbaud’s self-representation as a data security company, it has a deficient security program and no means to effectively manage or govern the data it holds. There are a number of known instances where Blackbaud maintained *unencrypted* Private Information. For example, the document ID field in Financial Edge NXT for I9 data was *not encrypted*.⁷² This

⁶⁹ *Id.* at 10.

⁷⁰ *Id.*

⁷¹ *Id.*

⁷² See *Blackbaud Cybersecurity Incident: You’re your Organization Needs to Know, Build Consulting*, <https://buildconsulting.com/learning/blackbaud-cybersecurity-incident-response-options/> (last visited Dec. 18, 2021) [<https://perma.cc/L4JN-86Q3>].

data field included, *inter alia*, SSNs, driver's license numbers, and passport numbers.⁷³ Additional *unencrypted* information, including credit card information, was also accessible from Raiser's Edge NXT and a system table from the Education Edge solution.⁷⁴ Blackbaud has also acknowledged that prior versions of its products, like Blackbaud CRM, stored *unencrypted* cardholder data.⁷⁵ Blackbaud also maintained *unencrypted* Private Information of some individuals on legacy versions of programs which were no longer in active use. Blackbaud knew this information was (a) unencrypted and thus subject to breach and misuse; (b) could not be seen by the Social Good Entities; (c) included highly sensitive PII; and (d) was "at rest," meaning the data was not in transit and being actively used. The failure to encrypt this "at rest" obsolete data containing highly sensitive PII on legacy and/or back-up versions of Blackbaud systems was particularly flagrant and egregious. There was no valid reason for retaining this highly sensitive PII, including SSNs, and Blackbaud's lax treatment of this PII made public exposure in a cyberattack very likely. Blackbaud has, in fact, acknowledged its failure to encrypt this highly sensitive PII which was "at rest," and only after the breach has it embarked on a program to encrypt such data.⁷⁶

352. [REDACTED] [REDACTED]
[REDACTED]

⁷³ *Id.*

⁷⁴ How are credit cards imported in version 7.91 and higher, Blackbaud, <https://kb.blackbaud.com/articles/Article/51196> (last visited Dec. 18, 2021) [<https://perma.cc/UWH4-6MWE>].

⁷⁵ PA DSS Implementation for Blackbaud CRM, Blackbaud, <https://www.blackbaud.com/files/support/guides/enterprise/400/padsscrm40sp7.pdf> (last visited Mar. 29, 2021) [<https://perma.cc/R3Q5-HCRK>].

⁷⁶ See Paul Colery, *Some Donor Data Accessed in Blackbaud Hack*, NonProfit Times (Sept. 29, 2020), https://www.thenonprofittimes.com/npt_articles/breaking-some-donor-data-accessed-in-blackbaud-hack/ [<https://perma.cc/2QRK-XWMK>].

[REDACTED] 77 [REDACTED]

[REDACTED] 78 [REDACTED]

- [REDACTED]

[REDACTED] 79

- [REDACTED]

[REDACTED] 80

- [REDACTED]

[REDACTED] 81

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] 82

⁷⁷ Friedberg Dep. at 213:22-214:6, 214:13-216:24, 219:4-10, 236:1-25, 246:5-247:2; PX20

⁷⁸ Friedberg Dep. at 213:22-214:6, 214:13-215:23; PX20

⁷⁹ Friedberg Dep. at 214:13-215:23; PX20.

⁸⁰ Friedberg Dep. at 215:5-23, 216:25-218:11; PX20.

⁸¹ Friedberg Dep. at 218:12-219:17; PX20.

⁸² Friedberg Dep. at 226:3-228:12; PX20 (emphasis added).

- [REDACTED]
- [REDACTED]
- [REDACTED] 83
- [REDACTED]
- [REDACTED]
- [REDACTED] 84
- [REDACTED]
- [REDACTED]
- [REDACTED] 85
- [REDACTED]
- [REDACTED]
- [REDACTED] 86
- [REDACTED]
- [REDACTED] 87
- [REDACTED]
- [REDACTED]
- [REDACTED] 88

⁸³ Friedberg Dep. at 216:6-11, 239:3-240:3, 247:10-248:4; PX20.

⁸⁴ Friedberg Dep. at 234:9-235:2; PX20.

⁸⁵ Friedberg Dep. at 218:12-219:3, 223:13-224:9; PX20.

⁸⁶ Friedberg Dep. at 242:24-244:3, 243:14-20, 245:1-246:4; PX20.

⁸⁷ Friedberg Dep. at 247:10-248:4; PX20.

⁸⁸ Friedberg Dep. at 248:5-21; PX20.

• [REDACTED]

89

353.

The image consists of eight horizontal black bars arranged vertically. The bars decrease in length from top to bottom. The top bar is the longest, followed by a shorter one, then another slightly shorter, and so on until the bottom bar is the shortest. All bars are set against a white background.

90

354.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] 9

355. Mr. Banda agreed

1

⁸⁹ Friedberg Dep. at 249:10-250:6; PX20.

⁹⁰ Banda Dep. at 225:23-226:24, 226:13-227:21, 227:23-228:3; PX20.

⁹¹ Banda Dep. at 230:16-231:10, 231:12; PX20 (emphasis added).

⁹² Banda Dep. at 231:13-16, 231:19; PX20.

356. Mr. Banda testified [REDACTED]

[REDACTED] [REDACTED]
[REDACTED]

357. [REDACTED]

⁹³ [REDACTED]

[REDACTED] ⁹⁴ [REDACTED]
[REDACTED]
[REDACTED] ⁹⁵

358. The data security component of Blackbaud's services is of great value to Social Good Entities, and the Social Good Entities pay a premium for this component of Blackbaud's services. Many of the Social Good Entities depend largely or wholly upon voluntary donations, and any concerns by donors as to the security of their Private Information can have significant adverse economic impacts, including a substantial decrease in donations. This is particularly true now, when many of the Social Good Entities are especially vulnerable on account of the widespread economic impacts of the ongoing pandemic.

359. At all relevant times, Blackbaud knew the Private Information stored on its computer systems was valuable and at risk of cyberattack. In its 2019 Annual Report, Blackbaud specifically acknowledged the risk of cyberattacks. Specifically, Blackbaud stated:

If the security of our software is breached, we fail to securely collect, store and transmit customer information, or we fail to safeguard confidential donor data, we could be exposed to liability, litigation, penalties and remedial costs and our reputation and business could suffer.

Fundamental to the use of our solutions is the secure collection, storage and transmission of confidential donor and end user data and transaction data, including in our payment services. Despite the network and application security, internal

⁹³ Friedberg Dep. at 149:4-11; 7/23/20 chat BLKB_MDL_00035993 at 8.

⁹⁴ *Id.* at 9.

⁹⁵ Friedberg Dep. at 99:4-21; PX11 at 6.

control measures, and physical security procedures we employ to safeguard our systems, we may still be vulnerable to a security breach, intrusion, loss or theft of confidential donor data and transaction data, which may harm our business, reputation and future financial results.⁹⁶

360. Further, Blackbaud acknowledged the sophistication of attacks and the need to constantly evaluate and adjust its procedures:

Like many major businesses, we are, from time to time, a target of cyber-attacks and phishing schemes, and we expect these threats to continue. Because of the numerous and evolving cybersecurity threats, including advanced and persistent cyber-attacks, phishing and social engineering schemes, used to obtain unauthorized access, disable or degrade systems have become increasingly more complex and sophisticated and may be difficult to detect for periods of time, we may not anticipate these acts or respond adequately or timely. As these threats continue to evolve and increase, we may be required to devote significant additional resources in order to modify and enhance our security controls and to identify and remediate any security vulnerabilities.⁹⁷

361. As such, Blackbaud identified the risk of failing to detect an attack and the consequences of such a failure, including a failure to respond adequately or on a timely basis. Additionally, Blackbaud identified risks inherent in a data breach and duties such a breach would trigger.

A compromise of our data security that results in customer or donor personal or payment card data being obtained by unauthorized persons could adversely affect our reputation with our customers and others, as well as our operations, results of operations, financial condition and liquidity and could result in litigation against us or the imposition of penalties. We might be required to expend significant capital and other resources to further protect against security breaches or to rectify problems caused by any security breach, including notification under data privacy laws and regulations and expenses related to remediating our information security systems. Even though we carry cyber-technology insurance policies that may provide insurance coverage under certain circumstances, we might suffer losses as a result of a security breach that exceed the coverage available under our insurance policies or for which we do not have coverage. A security breach and any efforts

⁹⁶ 2019 Form 10-K, *supra* n. Error! Bookmark not defined., at 20.

⁹⁷ *Id.*

we make to address such breach could also result in a disruption of our operations, particularly our online sales operations.⁹⁸

362. Although Blackbaud identified these risks as its own, it demonstrates an acute awareness of the adverse effects that could result from a data breach. Blackbaud recognized that it had a duty to keep Private Information secure.

Further, the existence of vulnerabilities, even if they do not result in a security breach, may harm client confidence and require substantial resources to address, and we may not be able to discover or remedy such security vulnerabilities before they are exploited, which may harm our business, reputation and future financial results.⁹⁹

363. The risk that data breaches and ransomware could cause to any business was well-known throughout the cybersecurity industry. The Identity Theft Resource Center identified ransomware as the “preferred method of data theft” by cyberthieves,¹⁰⁰ and the FTC cautioned businesses that developing a cybersecurity plan and educating employees is the best way to combat such attacks.¹⁰¹

364. The importance of developing a cybersecurity plan is more acute now than ever, as data breaches and ransomware attacks become more prevalent.¹⁰² Accordingly, Blackbaud was on notice of the harms that could ensue if it failed to protect individuals’ Private Information.

⁹⁸ *Id.*

⁹⁹ *Id.*

¹⁰⁰ *Identity Theft Resource Center 2020 Annual Report*, <https://notified.idtheftcenter.org/s/>.

¹⁰¹ *Cybersecurity for Small Business: Ransomware*, FTC, <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/ransomware> (last visited Mar. 28, 2021) [<https://perma.cc/DV2F-KGSJ>].

¹⁰² *Healthcare Data Breach Statistics*, HIPAA Journal, <https://www.hipaajournal.com/healthcare-data-breach-statistics/> (last visited Mar. 28, 2021) (“Our healthcare data breach statistics clearly show there has been an upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published.”) [<https://perma.cc/QDV2-ANMJ>].

365. Blackbaud itself knew that cyberattacks were a problem for businesses, and frequently informed its customers about the risks that companies faced as a result. Blackbaud recommended that its customers develop a “cybersecurity strategy that will combat cyberattacks and empower staff to become cyber security experts” to avoid the significant costs of data breaches:

**Fighting Cyber Crime:
It's Not Just a Job for IT**

Designed to access or destroy sensitive data, cyberattacks are an evolving danger to organizations. With millions of records stolen from data breaches every year, it's critical that your organization make cyber security a top priority—and this is not just a job for IT.

Employee users represent one of the most vulnerable links in the enterprise cyber security chain. Keep reading for tips on developing a cyber security strategy that will combat cyberattacks and empower staff to become cyber security experts.

63% of attacks use compromised credentials	146 is the median days an attacker is undetected on a network	\$500B is the potential cost of global cyber crime	\$3.8M is the average cost of data breach
--	---	--	---

*Source: Microsoft Threat Analytics

366. Blackbaud cautioned that its customers could face significant risk of the “exposure of data / personal identity information” in the event of a data breach, as well as the threat of ransomware. Blackbaud recommended that clients build out controls to guard against these risks.

¹⁰³ Fighting Cyber Crime: Its Not Just a Job for IT, Blackbaud (Sept. 2019), https://s21acms01blkbsa02.blob.core.windows.net/prod/docs/default-source/security/cyber-security.pdf?sfvrsn=61aa0bb_0 [https://perma.cc/TG46-C93M].

.....

Developing a Cyber Security Strategy

First, map out your threats and risks. Imagine what your worst-case scenario would look like. This could include theft of money (access to your bank accounts, wire fraud), exposure of data / personal identity information (student, donor, or employee records), availability of critical systems, theft of resources (for money), or ransomware.

Second, build out key controls. Now that you have a clear understanding of what you're trying to stop, lay out the controls that relate—combating phishing, protecting credentials, etc. Create initial controls against your top risks. For those that own or govern programs, leverage industry frameworks like the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF).

104

367. Based upon their significant expertise, Blackbaud warned consumers that managing data, knowing what data customers had, ensuring that vendors perform due diligence on their systems, and encrypting data were—among other things—the best way to safeguard data.

¹⁰⁴ *Id.*

7 Key Focus Areas to Optimize Your Efforts

A balance of people, process, and technology.

1. **Know What You Have** – Keep an inventory of what assets you have and where they live.
2. **Manage It Well** – Keep your support contracts active. Apply patches when vendors release them.
3. **Manage Access (and multifactor authentication (MFA))** – Limit who has access to your systems (especially critical or sensitive platforms). If you are compromised or phished, limit the exposure.
4. **Manage Data** – Know where your data is and ensure you're comfortable with those systems' methods of protection. Utilize encryption at rest and in transit.
5. **Build the Right Visibility** – Now that you know where your data is, do you have logs and records of who logged in and accessed it? Collect the data and ensure it is reviewed regularly.
6. **Manage Your Vendors** – Where vendors store or access your data, ensure you are performing due diligence on their security program. Sample questions to consider: Do they adhere to their compliance requirements? Do they have a security program that you are comfortable with? Do they share third party audit reports (e.g. SOC2/SSAE16)?
7. **Empower Your Staff** – Develop a policy & require acceptance. Communicate it and provide basic education. If possible, invest in a security awareness program.



“Companies spend millions of dollars on firewalls and secure access devices...none of these measures address the weakest link in the security chain: the people.”

—Kevin Mitnick, famous hacker

105

368. But Blackbaud’s customers, alone, could not ward off cyberattacks, and Blackbaud knew that a significant amount of the risk fell upon Blackbaud. Blackbaud anticipated that, even if it followed best practices, it could still be the subject of a data breach. Accordingly, Blackbaud developed an Incident Management and Response plan, and provided an overview to its customers.¹⁰⁶

¹⁰⁵ *Id.*

¹⁰⁶ *Blackbaud Cyber Security Incident Management and Response Overview*, Blackbaud (Feb. 2020), https://s21acms01blkbsa02.blob.core.windows.net/prod/docs/default-source/security/blackbaud_incident-management-and-response-overview.pdf?sfvrsn=15d418c6_0 [https://perma.cc/N9TL-4EBP]. *Blackbaud Cyber Security Incident Management and Response Overview*, Blackbaud (Feb. 2020), https://s21acms01blkbsa02.blob.core.windows.net/prod/docs/default-source/security/blackbaud_incident-management-and-response-overview.pdf?sfvrsn=15d418c6_0 [https://perma.cc/N9TL-4EBP].

369. In its Incident Management and Response Overview, Blackbaud noted that its chief concerns in the event of any data breach were to mitigate the impact and duration of a breach. In order to do so, preparation was key:

The objective of Blackbaud's Cyber Security Incident Response program is to promptly and effectively mitigate the *impact* and *duration* of a security relevant incident. In order to accomplish this, we believe much of the hard work occurs long before an incident is ever identified – proper *preparation*. We regularly test the incident response plan via regular tabletop exercises used to simulate potential attacks and response scenarios. This facilitates regular practice and continuously improves the incident response function. We also perform regular penetration testing to evaluate our preventative, detective, and responsive security capabilities.

107

370. Blackbaud's Incident Management and Response Overview focuses on the early identification of threats, notification “in a time frame that adheres to the latest compliance standards,” using security infrastructure in place to contain the threat, eradicating any of the tools or applications that a hacker used, restoring access to accounts, and performing “after-action” review to improve systems through detailed security analysis of the incident response.¹⁰⁸ Blackbaud’s practices do not include paying a ransom to mitigate damages associated with a data breach.

source/security/blackbaud_incident-management-and-response-overview.pdf?sfvrsn=15d418c6_0 [https://perma.cc/N9TL-4EBP].

¹⁰⁷ *Id.* at 2.

¹⁰⁸ *Id.* at 4.

371. Blackbaud was also aware of the risk that data breaches would pose by virtue of its understood obligations under foreign law. Blackbaud’s Privacy Shield Notice commits to maintaining “reasonable administrative, technical and physical safeguards to protect Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction.”¹⁰⁹ The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks are voluntary programs in which U.S. organizations may self-certify that they employ high data protection and security standards. The FTC enforces the Privacy Shield standards and encourages companies to “review their privacy policies to ensure they describe their privacy practices accurately.”¹¹⁰

372. Organizations that self-certify under the Privacy Shield Framework must “[d]evelop a Privacy Shield-[c]ompliant [p]rivacy [p]olicy [s]tatement”¹¹¹ that, among other things, must “inform individuals about . . . the types of personal data collected.”¹¹²

373. Blackbaud has self-certified to the Privacy Shield Framework, effective between August 1, 2016 and October 20, 2020.¹¹³ Blackbaud’s Privacy Shield Policy, submitted to the U.S.

¹⁰⁹ *Blackbaud Privacy Shield Certification Notice*, Blackbaud (Jan. 1, 2017), https://fundraising.blackbaud.co.uk/2017/01/01/blackbaud-privacy-shield-certification-notice/?_ga=2.190806440.2072851594.1616543868-605719626.1616543868 [<https://perma.cc/ZFW9-GP6L>].

¹¹⁰ *Update on the Privacy Shield Framework*, FTC (updated July 21, 2020), <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield> [<https://perma.cc/95ZB-3QLX>].

¹¹¹ *The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks* at 2, Int’l Trade Admin. <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdg> (last visited Mar. 24, 2021) [<https://perma.cc/HSA2-SVVL>].

¹¹² *1. Notice, Privacy Shield Framework*, Int’l Trade Admin. <https://www.privacyshield.gov/article?id=1-NOTICE> (last visited Mar. 24, 2021) [<https://perma.cc/MKW8-9Q4T>].

¹¹³ *Other Covered Entities, Privacy Shield Framework*, Int’l Trade Admin. Dec. 19, 2021 <https://www.privacyshield.gov/participant?id=a2zt0000000151AAA> (last visited Dec. 19, 2021) [<https://perma.cc/Y84V-FLNC>].

Department of Commerce and posted publicly on its website became effective August 1, 2016, and was last revised September 18, 2019.¹¹⁴

374. Blackbaud's Privacy Shield Notice also contains inaccuracies and unfair misrepresentations. Blackbaud's Privacy Shield Notice purportedly applies to Personal Data as follows:

For purposes of this Notice, "Personal Data" means information that (i) is transferred from the EEA or Switzerland to the United States, (ii) is recorded in any form, (iii) is about, or relates to, an identified or identifiable job applicant, consumer, customer, supplier or other individual (excluding Blackbaud employees), and (iv) can be linked to that job applicant, consumer, customer supplier or other individual.¹¹⁵

375. Blackbaud's Privacy Shield Notice commits to maintaining "reasonable administrative, technical and physical safeguards to protect Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction."¹¹⁶

376. Despite this commitment, Blackbaud did not protect Personal Data from unauthorized access during the Data Breach.

377. Further in its Privacy Shield Notice, Blackbaud states:

We do not collect sensitive Personal Data of consumers, customers or suppliers, such as information about medical or health conditions...political opinions, religious or philosophical beliefs...or other sensitive information as defined by the Privacy Shield framework.¹¹⁷

378. This statement is misleading and untrue. Blackbaud markets its "Grateful Patient Programs" ("GPPs"), which collects sensitive information, including medical and health

¹¹⁴ *Id.*

¹¹⁵ *Id.*

¹¹⁶ *Id.*

¹¹⁷ *Id.*

conditions, as well as its other “purpose-built patient engagement solutions”¹¹⁸ to U.K. and European healthcare organizations, including, *inter alia*, Operation Smile Ireland, Sarcoma UK, and St Columba’s Hospice.¹¹⁹

379. Blackbaud knew of the attendant risks that it and its customers faced as a result of hosting the Private Information of millions of individuals and determined that it, in the regular course of business, developing a robust cybersecurity program, including policies and building upon cybersecurity infrastructure were the best ways to prevent and recover from data breaches.

380. Because of the highly-sensitive and personal nature of Plaintiffs’ Private Information that Blackbaud collects and warehouses, Blackbaud has publicly affirmed its obligation and duty to secure Private Information.

C. Blackbaud’s Responsibility to Safeguard Information

381. Beyond the obligations created in its security and privacy policies, Blackbaud owed Plaintiffs and Class members a duty to safeguard their Private Information.

382. First, as described further below, Blackbaud owed a duty to safeguard Private Information pursuant to a number of statutes, including the HIPAA, the Federal Trade Commission Act (“FTC Act”), Children’s Online Privacy Protection Act (“COPPA”), to ensure that all information it collected and stored was secure. These statutes were intended to protect Plaintiffs and the Class members from the type of conduct by Blackbaud alleged herein.

383. Next, Blackbaud owed a duty to safeguard Private Information given that it was on notice that it was maintaining highly-valuable data, for which Blackbaud knew there was a risk

¹¹⁸ *Healthcare Organisations*, Blackbaud, <https://www.blackbaud.co.uk/who-we-serve/healthcare-organisations> (last visited Dec. 19, 2021) [<https://perma.cc/W77C-XG8E>].

¹¹⁹ *Customer Stories*, Blackbaud, <https://www.blackbaud.co.uk/customer-stories> (last visited Dec. 19, 2021) [<https://perma.cc/VY5F-65NJ>].

that it would be targeted by cybercriminals. Blackbaud knew of the extensive harm that would occur if Plaintiffs' and Class members' Private Information were exposed through a Data Breach, and thus owed a duty to safeguard that information.

384. Given the sensitive nature of the Private Information obtained by the Social Good Entities, Blackbaud knew that hackers and cybercriminals would be able to commit identity theft, financial fraud, phishing, socially-engineered attacks, healthcare fraud, and other identity-related fraud if it were able to exfiltrate that data from Blackbaud's servers. Blackbaud also knew that individuals whose Private Information was stored on Blackbaud's servers would be reasonable in spending time and effort to mitigate their damages and prevent identity theft and fraud if that data were exfiltrated.

385. Blackbaud also owed a duty to safeguard Plaintiffs' and Class members' data based upon the promises that it made to its customers to safeguard data, as well as the disclosures that it made in its data security policies and privacy policies. Blackbaud voluntarily undertook efforts to keep that data secure as part of its business model and thus owes a continuing obligation to Plaintiffs and Class members to keep their Private Information secure.

386. Blackbaud also owed a duty to comply with industry standards in safeguarding Private Information, which—as discussed herein—it did not do.

D. Blackbaud Failed to Meet Its Obligations to Protect Private Information or Comply with its own Privacy Policies

387. Blackbaud's services are supported by privacy policies and security practices, which it provides on a publicly-facing website.

388. Blackbaud was keenly aware of the obligations that state and federal law imposed upon it given the types of information that Blackbaud stored and processed for Social Good Entities.

Driving social good on a global scale—spanning the public, private, and social sectors—requires a detailed understanding of privacy standards. Blackbaud has dedicated legal counsel who continually evaluate upcoming and changing regulations as they relate to data privacy to ensure we are aligned to these regulations, as well as providing thought leadership for our customers on the operational impact of these regulations and compliance requirements.

We were also an early adopter of the EU-US Privacy Shield, which is intended to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring data between the EU, the U.K., Switzerland, and the United States.

Blackbaud is committed to providing products and services that enable customers to comply with the privacy laws applicable to them. We tirelessly track and interpret pending legislation to ensure that Blackbaud provides the features you need to protect the privacy of your constituents while managing data in a compliant way. As privacy legislation evolves, our products do too. Further, we will continue to work on ways to improve the user experience in the products, specifically as regards the capture, recording, and use of your supporters' consent. We ensure that (when applicable) our products and internal processes comply with and enable customers to comply with:

- General Data Protection Regulation (GDPR): A European Union regulation that establishes commercial standards for data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA)
 -
- Health Insurance Portability and Accountability Act (HIPAA): A U.S. law that provides data privacy and security provisions for safeguarding Protected Health Information (PHI).
 - Blackbaud regularly performs assessments for our compliance with industry-standard data protection protocols such as HIPAA.
 - All Blackbaud products available to customers in the healthcare sector are assessed for compliance with HIPAA compliance annually. Additionally, these products are also reviewed to ensure customers can achieve and maintain their own HIPAA compliance obligations when performing fundraising and data management activities using Blackbaud solutions.
- California Consumer Privacy Act (CCPA): a U.S. bill that enhances privacy rights and consumer protection for residents of California.
 - As of the effective date of the California Consumer Privacy Act (CCPA), Blackbaud will be fully compliant with this law.
 - Similar to the guidance provided on GDPR, prior to the effective date of the CCPA, Blackbaud will issue guidance on how our

various solutions can be used for our customers to help them comply with these regulations

We understand regulatory requirements and constituent expectations around data privacy are a key priority for our customers as well. For more information about safeguarding your constituent data, reference the Blackbaud Institute's Privacy Toolkit.¹²⁰

389. Blackbaud also had a special relationship with Plaintiffs and Class members from being entrusted with their Private Information, which provided an independent duty of care. Blackbaud had a duty to use reasonable security measures because it undertook to collect, store and use consumers' Private Information. Regardless of whether an individual entered their information through Blackbaud's website (such as on a hosted form for a charitable entity), or the information was provided to Blackbaud by a Social Good Entity as part of a servicing agreement, Blackbaud owed a duty to protect and safeguard that Private Information. Blackbaud's contention in a recent SEC filing that "plaintiffs lack contractual privity with us"¹²¹ misses the point.

390. Blackbaud has further failed Plaintiffs and Class members by its failure to maintain a comprehensive and sufficient security program, including by not adequately securing and protecting Private Information that was stored on outdated legacy tables or files stored on Blackbaud's systems that no longer had a reasonable or practicable business purpose, which, as proven by the Data Breach, were exposed and vulnerable to hacking and theft.

391. Blackbaud failed to provide Plaintiffs and Class Members with timely and adequate notice of the extent of the Data Breach by falsely assuring them in its public statements and Notices issued prior to September 29, 2020, that the attack only impacted certain Private Information and

¹²⁰ Your Security is Our Priority (Mar. 2, 2020), Blackbaud <https://web.archive.org/web/20200302212750/> <https://www.blackbaud.com/security>.

¹²¹ Blackbaud, Inc., Form 10-Q at 20 (Nov. 3, 2020), <https://investor.blackbaud.com/static-files/b861e404-fa85-4f5b-a833-bc30de0165dd>.

specifically did not include SSNs. Timely notification of the breach was required so that, among other things, Plaintiffs and Class members could take measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to try to prevent identify theft.

392. Remarkably, Blackbaud President and CEO, Mike Gianoni, told *The NonProfit Times* that Blackbaud had “no reason to believe it [the Data Breach] will result in any public disclosure of any of our customers’ data.”¹²²

393. The duty to protect Plaintiffs’ Private Information is non-delegable, particularly here where Blackbaud’s entire business model is premised upon voluntarily assuming the duty by soliciting customers to utilize its professed ability to manage, house, and safeguard data. Accordingly, Blackbaud is liable to Plaintiffs and the Class or the compromise and unauthorized disclosure of their Private Information.

E. Blackbaud Failed to Comply with Industry and Regulatory Standards

394. Because of the value of PII and PHI to hackers and identity thieves, companies in the business of storing, maintaining and securing Private Information, such as Blackbaud, have been identified as being particularly vulnerable to cyber-attacks. Cybersecurity firms have promulgated a series of best practices that at minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management

¹²² Colery, *supra* n.23.

systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.¹²³ Indeed, Blackbaud recognizes these best practices, and discusses many of them in its security and privacy protocols and policies.

395. Additionally, part of a company's cybersecurity hygiene concerns the ability to patch software and ensure that older databases and servers remain secure. According to Confidential Witness No. 1, the databases that were impacted by the Data Breach were older, and "one of the last vestiges" of Blackbaud's old data center.

396. Further, federal and state governments have likewise established security standards and issued recommendations to diminish data breaches and the resulting harm to consumers and financial institutions. The FTC has issued numerous guides for business highlighting the importance of reasonable data and cyber security practices. According to the FTC, the need for data and cyber security should be factored into all business decision-making.¹²⁴

397. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data and cyber security principles and practices for business.¹²⁵ The guidelines note businesses should protect the personal customer and consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's

¹²³ See *Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, Inc. (Nov. 2016), <https://insights.datamark.net/addressing-bpo-information-security/> [<https://perma.cc/NY6X-TFUY>].

¹²⁴ *Start with Security: A Guide for Business* at 2, FTC (June 2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

¹²⁵ *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business> [<https://perma.cc/9945-U4HV>].

vulnerabilities; and implement policies to correct security problems.¹²⁶ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.¹²⁷

398. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

399. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer and consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data and cyber security obligations.

400. Blackbaud also has obligations created by other federal and state law and regulations, contracts, industry standards, and common law to maintain reasonable and appropriate physical, administrative, and technical measures to keep Plaintiffs' and Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

¹²⁶ *Id.*

¹²⁷ *Id.*

401. Blackbaud was no stranger to following stringent security and privacy policies. Upon information and belief, as a government contractor for, *inter alia*, the Department of the Army, the Department of State, the Department of Veterans Affairs, and the Smithsonian Institution, Blackbaud is subject to cyber security obligations stemming from federal law, such as the Privacy Act of 1974, as amended, 5 U.S.C. § 552a, and 48 C.F.R. § 52.204-21.¹²⁸

402. Blackbaud also had a duty to safeguard Plaintiffs' and Class members' PHI under HIPAA and its implementing regulations, 45 C.F.R. §§ 160, *et seq.*, which establish privacy and security standards for certain health organizations and their "business associates." *See id.* § 164.302. Blackbaud is a "business associate" subject to HIPAA because it receives, maintains, or transmits its customers' PHI. *Id.* § 160.103. "PHI" includes, in relevant part, individually identifiable health information relating to the provision of health care, such as Plaintiff Clayton's compromised medical data. *Id.*

403. For example, HIPAA required Blackbaud to ensure the confidentiality of the electronic PHI it received and maintained by protecting against reasonably anticipated threats to its integrity. *Id.* § 160.306(a). To do so, Blackbaud was required to implement reasonable and appropriate security measures to mitigate the risk of unauthorized access to its customers' electronic personal health information, including by encrypting certain data where appropriate. *See id.* §§ 164.308 (administrative safeguards), 164.312 (technical safeguards).

404. Blackbaud similarly violated other statutes by failing to implement reasonable security measures to mitigate the risk of unauthorized access, and encrypting necessary information.

¹²⁸ Darren Death, *Information Security Requirements for U.S. Federal Contractors*, Forbes (Sept. 4, 2018), <https://www.forbes.com/sites/forbestechcouncil/2018/09/04/information-security-requirements-for-u-s-federal-contractors/#4c0c6b83451b> [https://perma.cc/CMN2-9YLM].

405. Given the magnitude of the risk and repercussions of a breach or attack targeting this type of data, the likelihood of a breach or attack, and Blackbaud's explicit awareness of these vulnerabilities, Blackbaud should have taken every reasonable precaution in developing a robust security program and protecting Plaintiffs' and the Class members' Private Information. However, Blackbaud failed to even employ "appropriate" safeguards as it pledged in its Privacy Policy, leaving the sensitive Private Information in its possession exposed to unauthorized access. This is especially concerning since Blackbaud serves many non-profit organizations, which depend on donor contributions such as those of Plaintiffs to fund their operations, and ultimately allowed the donors' data to be compromised and misused.

406. Despite its duties, representations, and promises, Blackbaud failed to adequately secure and protect its clients' data, including that of the numerous non-profits, such as the respective organizations which maintained Plaintiffs' and the Class members' Private Information, allowing the Private Information to be accessed, disclosed, and misused.

F. Blackbaud's Failures Resulted in a Data Breach

407. In February of 2020, an unknown attacker intruded onto the Blackbaud network. They used [REDACTED]¹²⁹ On March 3, 2020, [REDACTED]
[REDACTED]

¹²⁹ Friedberg Dep. at 47:25-48:14; PX8 at 16.

[REDACTED]

[REDACTED]

408.

[REDACTED] 130 [REDACTED]

[REDACTED] 131

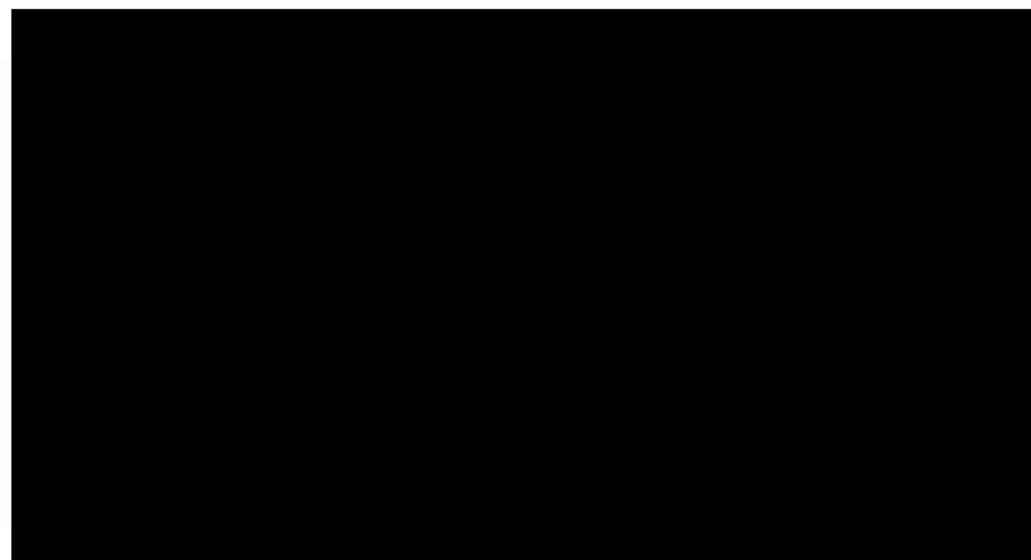
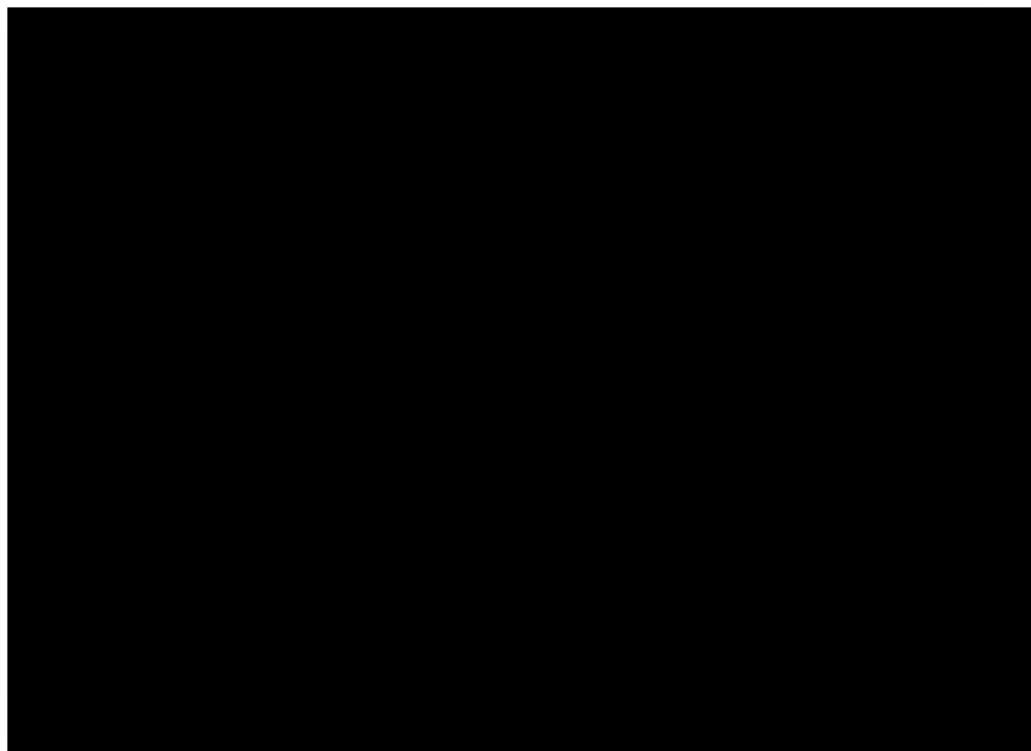
409.

[REDACTED] 132

¹³⁰ Friedberg Dep. at 72:16-73:5, 76:17-24; PX9 at 3, 4.

¹³¹ Friedberg Dep. at 72:16-73:5; PX9 at 2-5.

¹³² Friedberg Dep. at 42:7-16, 121:10-23, 158:23-159:10; PX12; PX11 at 13; PX14; PX14 at 16.



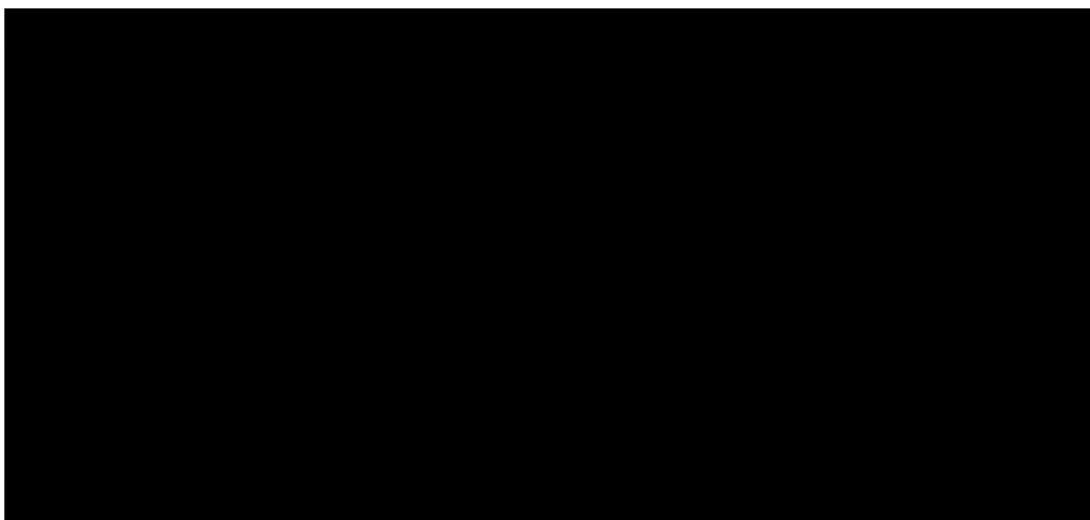
410. [REDACTED]

[REDACTED]

[REDACTED] 133 [REDACTED]

[REDACTED] 134 [REDACTED]

[REDACTED] 135



411. [REDACTED]

[REDACTED]
[REDACTED]

412. [REDACTED]

[REDACTED] 136 [REDACTED]

133 [REDACTED]

Friedberg Dep. at 33:6-34:20, 263:20-264:2, 267:21-268:18; PX22; PX23 at 7.

134 Friedberg Dep. at 104:22-105:10; PX11 at 9 [REDACTED]

135 Friedberg Dep. at 264:3-265:20; PX22 at 7.

136 Friedberg Dep. at 137:20-138:18; PX13 at 6.

[REDACTED]
[REDACTED] 137

413. [REDACTED] [REDACTED]

[REDACTED] 138

414. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED]
[REDACTED] 139 [REDACTED]
[REDACTED]

415. [REDACTED]

¹³⁷ Friedberg Dep. at 46:25-47:4, 143:12-144:11; PX13 at 1.

¹³⁸ PX19 or [REDACTED]
[REDACTED]

¹³⁸ Friedberg Dep. at 192:23-193:10, 193:11-1949:9; PX17 at 3 [REDACTED]

¹³⁸ Friedberg Dep. at 163:11-164:1; PX15 at 2(noting the [REDACTED]
[REDACTED])

¹³⁸ Friedberg Dep. at 173:9-174:13, 174:18-175:14; PX16 at 2.

¹³⁸ Friedberg Dep. at 209:1-13.

¹³⁹ Friedberg Dep. at 192:23-193:10, 193:11-1949:9; PX17 at 3 (recommending [REDACTED]
[REDACTED] and 18 (recommending [REDACTED]).

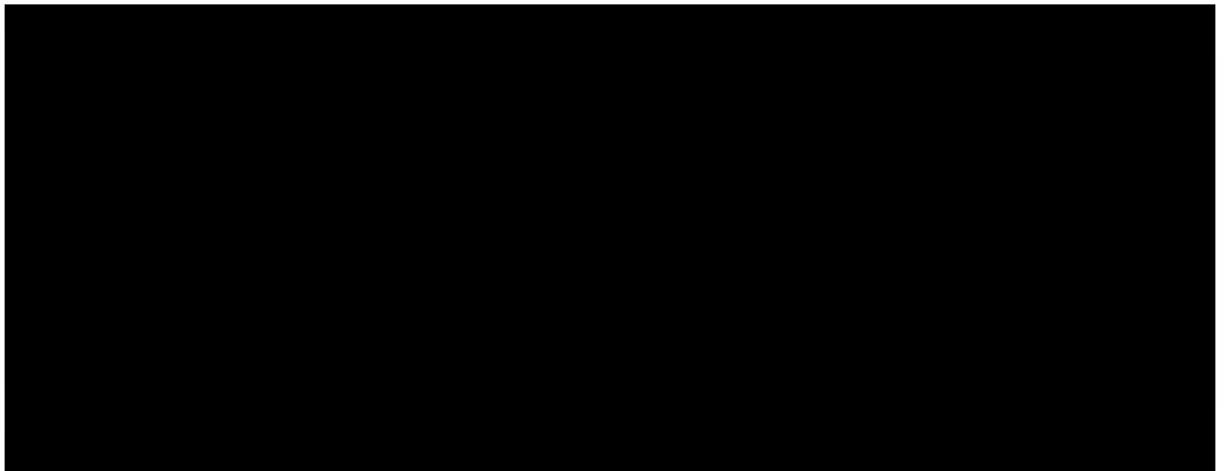
[REDACTED] 140 [REDACTED]

[REDACTED] 141

416. [REDACTED]

[REDACTED] 142 [REDACTED]

[REDACTED] 143 [REDACTED]



417. [REDACTED]



[REDACTED] 144

¹⁴⁰ Friedberg Dep. at 163:11-164:1; PX15 at 2(noting the [REDACTED]
[REDACTED])

¹⁴¹ Friedberg Dep. at 173:9-174:13, 174:18-175:14; PX16 at 2.

¹⁴² Friedberg Dep. at 209:1-13; PX18 at 6-7, and 8 (stating [REDACTED])

See also Friedberg Dep. at

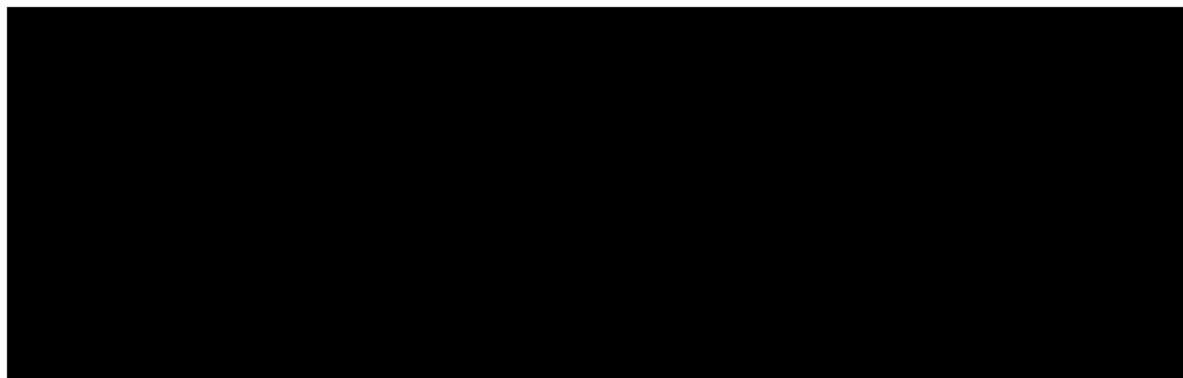
213:6-12 (noting [REDACTED])

¹⁴³ BLKB_MDL_00195062 at 2.

¹⁴⁴ Friedberg Dep. at 46:16-24.

418. [REDACTED]

[REDACTED] 145



419. [REDACTED]



[REDACTED] 146

420. Prior to the ransomware attack and Data Breach, Plaintiffs and Class members provided sensitive and personally identifying Private Information to Blackbaud as part of their participation in fundraising by non-profit companies, seeking healthcare from healthcare providers, seeking education from K-12 school providers and universities, and/or seeking other services from Blackbaud's clients, the Social Good Entities. When providing such information, Plaintiffs and Class members reasonably expected that the manager and securer of their Private Information, Blackbaud, would maintain security against cybercriminals and cyberattacks.

421. Blackbaud maintained Plaintiffs' and the Class members' data on a shared network, server, and/or software. Despite its own awareness of steady increases of cyberattacks on health

¹⁴⁵ PX10 at 2.

¹⁴⁶ Friedberg Dep. at 239:24-240:3, 240:23-241:8, 245:24-246:4, 247:5-248:4, 248:11-21, 253:16-254:11; PX20; PX21 at 35-36.

care providers, schools, and other facilities over the course of recent years, Blackbaud did not maintain adequate security of Plaintiffs' and the Class members' Private Information, and did not adequately protect it against hackers and cyberattacks.

422. Blackbaud maintained Private Information on servers that were obsolete. According to Confidential Witness No. 1, the servers were not on the system patch schedule and were "forgotten machines."

423. According to Confidential Witness No. 1, Blackbaud had planned on upgrading the old servers to new technology. The servers that were breached were one of the last environments to be rolled over onto a new platform that Blackbaud was implementing called "Raiser's Edge." The older servers, according to Confidential Witness No. 1, were operating multiple applications, and Blackbaud wanted to eventually merge them onto a new, base application on one server. According to Confidential Witness No. 1, upgrading to new technology had been "on a laundry list for a while."

424. According to Confidential Witness No. 1, employees at Blackbaud became increasingly alarmed with Blackbaud's failure to patch old systems, and even eventually emailed executives about the vulnerabilities—receiving a response from one executive: "we're working on it."

425. Confidential Witness No. 1 also warned Blackbaud about process vulnerabilities that would subject them to attack—such as using remote desktop access and the vulnerabilities that had been uncovered in security scans. According to Confidential Witness No. 1, the remote desktop access configuration was particularly concerning for a year leading up to the data breach—so much so that they and their team members would simply "shut down the machines" because they knew the risk was too high to allow them to continue to operate.

426. In addition to the emails that Confidential Witness No. 1 and their team sent to executives, prior to the breach they separately advised that Crowdstrike needed to be installed on Blackbaud’s machines to capture logs, including the logs that were later erased by the ransomware in this case. Because Blackbaud elected not to install a program on their servers that would have assisted in the forensic investigation of the Data Breach, the data that would normally be used in a forensic investigation is limited. To be clear: Blackbaud elected to not have this functionality and, as a result, the data on the Data Breach is limited.

427. The ransomware attack that began in February 2020 and continued until May 2020, led to the removal of one or more copies of some or all of the accessed data. Once removed, the hackers could easily have re-copied the stolen data.¹⁴⁷ The ransomware attack was twofold: the cybercriminals copied data from the systems and held it for ransom, and upon being discovered, the cybercriminals attempted but allegedly failed to block Blackbaud from accessing its own systems.¹⁴⁸

428. The first paragraph of Blackbaud’s notice about the Data Breach on its website dated July 16, 2020 (the “Website Notice”), does not inform Class members about the true nature of the sensitive Private Information exfiltrated by the hackers; rather, it seeks to normalize hacking and paint Blackbaud as both a victim and a hero, stating:

The Cybercrime industry represents an over trillion-dollar industry that is ever-changing and growing all the time—a threat to all companies around the world. Like many in our industry, Blackbaud encounters millions of attacks each month, and our expert Cybersecurity team successfully defends against those attacks while constantly studying the landscape to stay ahead of this sophisticated criminal

¹⁴⁷ Gary Guthrie, *Paying to delete stolen data doesn’t always work out for the victim, new study suggests*, ConsumerAffairs, <https://www.consumeraffairs.com/news/paying-to-delete-stolen-data-doesnt-always-work-out-for-the-victim-new-study-suggests-110520.html> (last visited Dec. 19, 2021) [<https://perma.cc/DMV2-JRFP>].

¹⁴⁸ See *Learn More Announcement*, *supra* n.6.

industry. We wanted to notify our customers and other stakeholders about a particular security incident that recently occurred.¹⁴⁹

429. In fact, Blackbaud's Website Notice devotes only three of 20 sentences to describing the impact the Data Breach might have on its Class members, withholding critical details from the public that would have allowed Plaintiffs and Class members to assess the risks to their Private Information and take targeted, but reasonable, precautionary protective measures based on the nature of the incident.

430. Blackbaud stated in its Website Notice that it initially discovered a ransomware attack in May of 2020¹⁵⁰ that attempted to "disrupt the business by locking companies out of their own data and servers."¹⁵¹ According to Blackbaud's statement:

After discovering the attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system. Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. **The cybercriminal did not access credit card information, bank account information, or social security numbers.** Because protecting our customers' data is our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. . . . The subset of customers who were part of this incident have been notified and supplied with additional information and resources. We apologize that this happened and will continue to do our very best to supply help and support as we and our customers jointly navigate this cybercrime incident.¹⁵²

¹⁴⁹ *Id.*

¹⁵⁰ *Security Incident*, Blackbaud (July 19, 2020), <https://www.blackbaud.com/securityincident> [<https://web.archive.org/web/20200719170537/https://www.blackbaud.com/securityincident>].

¹⁵¹ *Id.*

¹⁵² *Id.* (emphasis added). Notably, the language in bold has since been removed. *See also Security Incident*, Blackbaud (updated Sept. 29, 2020), <https://www.blackbaud.com/securityincident> (last visited Dec. 19, 2021) [<https://perma.cc/MB7C-YUAR>].

431. Overall, Blackbaud’s Website Notice raised more questions about the impact to Class members than it answered. For example, Blackbaud’s Website Notice did not:

- a. disclose the size of the Data Breach (an unspecified “subset” of individuals were impacted);
- b. explain why Blackbaud waited approximately two months to notify authorities of the Data Breach after the ransomware attack was detected;
- c. explain how the hackers gained access to Blackbaud’s system (*e.g.*, via phishing or an exploit kit);
- d. explain the nature of the “confirmation” that the copy of the data the cybercriminals removed “had been destroyed;”
- e. explain what specific facts cause Blackbaud to believe that the exfiltrated data will not be misused by the individuals who stole it, despite those individuals having already proven to be criminal by their actions;
- f. explain what specific changes Blackbaud “implemented . . . to prevent this specific issue from happening again” or what vulnerabilities the attack exposed that needed to be remediated; or
- g. say whether the method is used to “prevent[] the cybercriminal from blocking our system access and fully encrypting [our] files” was actually the payment of a ransom to the cybercriminals.¹⁵³

432. Blackbaud’s opaque data breach announcement has left Plaintiffs and Class members with more questions than answers. Blackbaud’s lack of transparency means that Plaintiffs and Class members still do not know how Blackbaud restricted access to Private Information or the extent to which it practiced cybersecurity hygiene, such as data minimization or deleting data after a certain period of time. Similarly, Blackbaud has completely failed to provide basic information about the Data Breach, itself, to the public—including when it was actually first detected; what Private Information was compromised, accessed, and exfiltrated; which security and privacy practices were insufficient (or not followed) so as to allow the Data Breach to occur; what Blackbaud is doing to prevent future data breaches; what representations were made by the cybercriminals during the ransom negotiations; and how can Blackbaud be

¹⁵³ *Id.*; *Learn More Announcement*, *supra* n.6.

assured that the cybercriminals will not target the individuals whose Private Information was taken.

433. Blackbaud's lack of clarity about the extent of the information that was comprised, has left Plaintiffs and Class members to fend for themselves, spending time, effort, and money to protect themselves in the wake of the Data Breach.

434. Both the Security Incident and blog pages on Blackbaud's website are devoid of any explanation to the affected individuals as to how they could protect themselves with credit freezes, credit monitoring, or other action.

435. Although Blackbaud originally claimed in its Website Notice that credit card information and bank account information was not accessed, from August 17, 2020 through September 3, 2020, many Social Good Entities warned individuals that their sensitive data, including SSNs and payment information, may actually have been accessed.¹⁵⁴

436. Plaintiffs received notices advising individuals whose Private Information was accessed to, *inter alia*, "remain vigilant over the next twelve to twenty-four months for any strange inquiries, including potential phishing attempts," and report "any suspicious activity or suspected identity theft." Furthermore, one Notice furnished to Plaintiff Case advised that the organization

¹⁵⁴ See, e.g., Notice Letter from University of Detroit Mercy, <https://oag.ca.gov/system/files/9028629.PDF> (warning that cybercriminals may have accessed individuals' full name and SSN) [<https://perma.cc/4QU8-SSBY>]; [bigthought.org, Blackbaud Security Breach and How it Affects You, Your Privacy, and Big Thought](https://www.bigthought.org/blackbaud-security-breach-and-how-it-affects-you-your-privacy-and-big-thought), Big Thought <https://www.bigthought.org/announcements/news-announcements/blackbaud-security-breach-and-how-it-affects-you-your-privacy-and-big-thought/> (last visited Dec. 19, 2021) ("Although Blackbaud has stated that all information was encrypted, a social security number or employment identification number (EIN) may have been accessible to the cybercriminal...") [<https://perma.cc/H7AR-R7ED>]; *56,000 Northwestern Memorial HealthCare Donors Impacted by Blackbaud Ransomware Attack*, HIPAA Journal, <https://www.hipaajournal.com/56000-northwestern-memorial-healthcare-donors-impacted-by-blackbaud-ransomware-attack/> (last visited Dec. 19, 2021) (noting that the database contained the SSNs and/or financial payment card information of individuals) [<https://perma.cc/VV8K-YVVE>].

“cannot be completely certain” that Blackbaud was indeed able to retrieve the stolen data. In at least one other notice, the institution advised that it was “examining our vendor relationship with Blackbaud and evaluating their security safeguards.”

437. Blackbaud originally (and falsely) reported that no SSNs, bank account information, or other financial data was compromised. For example, Plaintiff Glasper received a notice from Allina Health informing him that the information that could have been accessed “DID NOT include: [c]redit card information, [b]ank account information, Social [S]ecurity numbers, [and] [a]ny additional medical information, such as diagnosis or treatment plan.”

438. Blackbaud’s defective notice further increased the likelihood of harm to Plaintiffs and Class members by suggesting that the Social Good Entities were “unlikely” to have data breach notification obligations to their students, patients, constituents, and donors.¹⁵⁵ This improper suggestion may have caused some Social Good Entities to delay notifying Class members and some to never be notified at all.

439. As a result of Blackbaud’s lax data protection standards, cybercriminals obtained access not only to recently-obtained information, but Private Information that remained on backup files for years, if not decades. For example, one Notice warned “we cannot determine with certainty that the [i]nformation will not be misused.” This Notice also advised that “[u]nfortunately, the cybercriminal removed a copy of the backup files of many of its customers, including our backup file that may have contained your personal information.”

¹⁵⁵ Letter from Anjali Das, att’y at Wilson Elser Moskowitz Edelman & Dicker LLP, to Wayne Stenehjem, North Dakota Att’y Gen., at PDF p. 5 (Sept. 14, 2020), <https://attorneygeneral.nd.gov/sites/ag/files/documents/DataBreach/2020-09-14-LakesPrairiesCAP.PDF> [<https://perma.cc/9SWK-R8J7>].

440. Moreover, Blackbaud's initial assurances that SSNs and other sensitive data had not been accessed ultimately proved false. As late as September 14, 2020, as reflected in a letter from an attorney representing not-for-profit Lakes & Prairies Community Action Partnership, Blackbaud had provided assurances that SSNs and other "sensitive text fields" on Blackbaud's *Financial Edge* platforms, even in back-up data, were encrypted. However, in September and October 2020, Blackbaud informed certain of its customers that, in fact, such information had been compromised—and, shockingly, this breach occurred in some instances because Blackbaud had maintained much of this sensitive Private Information for decades without encryption, making it particularly vulnerable to theft. Plaintiff Roth received a Notice from his children's former school that stated "Blackbaud indicated that certain information previously believed to have been encrypted was subsequently determined . . . to not have been encrypted, and that the compromised file may have contained your full name, Social Security number, date of birth, and address."

441. The Data Breach was the result of Blackbaud's failure not only to properly and adequately determine whether it was susceptible to a data breach but also its negligent and reckless failure to remove old unused and obsolete data containing Private Information or to encrypt such information. Blackbaud, in fact, had no valid business reason for retaining such records containing highly sensitive Private Information—including SSNs—for such long periods and for failing to delete or encrypt such information. For example, the letter from Blackbaud to one of its educational institution customers impacted by the Data Breach stated that SSNs of former students and their parents, as well as faculty members, were exposed on unused tables in a legacy version on Blackbaud's systems.

442. Remarkably, Blackbaud's retention of this Private Information in unencrypted form on older legacy versions of its programs made public exposure of such data in a cyberattack very

likely. It is particularly egregious that Blackbaud continued to keep legacy versions of the software on its systems, despite the fact that, by the time of the Data Breach, there was no valid business reason to continue to maintain this information on its systems. The failure was knowing, reckless and, at bare minimum, negligent given the known risks to Blackbaud—particularly given vendor announcements regarding the sunset of certain databases and Blackbaud’s failure to move Private Information to newer systems with more robust security features. The breach of Plaintiffs and Class members’ Private Information, particularly their SSNs, is a direct consequence of this conduct.

443. Accordingly, Blackbaud’s statements of reassurance were unfounded, particularly in light of Blackbaud’s earlier admission to the SEC that: “further forensic investigation found that for some of the notified customers, the cybercriminal may have accessed some unencrypted fields intended for bank account information, [S]ocial [S]ecurity numbers, usernames and/or passwords.”¹⁵⁶

444. Blackbaud did not have a sufficient security program in place to prevent cyberattack and access, which is evident by its own statements after the Data Breach that it has “already implemented changes to prevent this specific issue from happening again.”¹⁵⁷

445. This discovery was the result of an internal investigation and subsequent Forensic Report (the “Report”),¹⁵⁸ which shows that even Blackbaud’s investigation into the Data Breach was insufficient. The Report notes that [REDACTED]

¹⁵⁶ Sept. 2020 Form 8-K, *supra* n.36, at 2.

¹⁵⁷ *Learn More Announcement*, *supra* n.6.

¹⁵⁸ Kudelski Security, Blackbaud Incident Report (July 14, 2020), BLKB_MDL_00000001.

[REDACTED], and does not address the full scope of the Data Breach.¹⁵⁹ It also is [REDACTED]
[REDACTED]
[REDACTED].

446. Blackbaud's report also highlights the steps it could have taken—but failed to take—to prevent the Data Breach. For example, the Report notes that the [REDACTED]

[REDACTED] was utilized to develop a “real-time telemetry of the attacker’s actions against multiple systems.”¹⁶⁰ Had Blackbaud utilized [REDACTED] in its regular course of business, or employed other measures as many other data management firms do, it might have been able to prevent or stop the Data Breach.

447. The acknowledged types of data exposed included Plaintiffs’ Private Information, including Plaintiffs’ and Class members’ names, addresses, phone numbers, email addresses, dates of birth, and/or SSNs. Blackbaud’s Report states that analysis was “unable to detect credit card data while reviewing exfiltrated data,” and improperly concludes that no credit card data was exfiltrated, although such data could have existed in the unexamined database files.¹⁶¹

448. Blackbaud’s reliance on the word of cybercriminals or a “certificate of destruction” issued by those same thieves that the “copied” or stolen subset of any data was destroyed is patently unreasonable. Blackbaud has not and cannot be assured that SSNs, bank account numbers, and credit card numbers were not also accessed and retained by the cybercriminals, particularly insofar as it advised its clients to inform affected individuals to monitor accounts for suspicious activity and/or identity theft.

¹⁵⁹ See *id.* at 7. The Report does not make clear whether Blackbaud identified these systems itself, or whether another firm was engaged to determine what systems were affected by the Breach.

¹⁶⁰ *Id.* at 2.

¹⁶¹ *Id.* at 2.

449. In fact, Blackbaud's CISO, among other Blackbaud employees, [REDACTED]
[REDACTED]

Despite recognizing the need for ongoing monitoring due to significant heightened risk, Blackbaud has offered no remuneration in the event of actual identity theft or misuse. Further, Blackbaud's misrepresentations to the public regarding [REDACTED] remains on its website and continues to mislead the public regarding facts that may dictate what actions are needed to protect themselves from misuse of their Private Information. In addition to damages and injunctive relief, Plaintiffs have brought this litigation for Blackbaud to correct its misstatements.

450. Likewise, reputable third parties have questioned the reasonableness of Blackbaud's faith in the cybercriminals and encouraged those individuals impacted by the Data Breach to take measures to protect against targeted future criminal activity.¹⁶² For example, the Michigan Attorney General's office rejected Blackbaud's reliance on the promises of cybercriminals, noting that "Blackbaud claims that it has 'no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly' but, to date, has not announced any concrete substantiation of this claim."¹⁶³

¹⁶² Leo Kelion & Joe Tidy, *National Trust Joins Victims of Blackbaud Hack*, BBC News (July 30, 2020), <https://www.bbc.com/news/technology-53567699> ("Although Blackbaud has said the cyber-criminals had provided confirmation that the stolen data was destroyed, one expert questioned whether such an assurance could be trusted. 'The hackers would know these people have a propensity to support good causes,' commented Pat Walshe from the consultancy Privacy Matters. This would be valuable information to fraudsters, he added, who could use it to fool victims into thinking they were making further donations when in fact they would be giving away their payment card details.") [<https://perma.cc/NC7W-T9LJ>].

¹⁶³ *Phishing Scams Following Blackbaud Security Breach*, Mich. Dep't Att'y Gen., https://www.michigan.gov/ag/0,4534,7-359-81903_20942-540014--,00.html (last visited Dec. 19, 2021) [<https://perma.cc/E6K9-HVZZ>].

451. The FBI recognizes the likelihood that cybercriminals will renege on their promises once a ransom is paid, stating that it “does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data.”¹⁶⁴ Several media outlets and industry groups have likewise questioned reliance on promises by cybercriminals.¹⁶⁵ Additionally, many Social Good Entities’ own Data Breach notices rightly advise affected individuals to monitor their own credit and financial accounts for suspicious account activity and notify the Social Good Entity of any such activity.¹⁶⁶ [REDACTED]

[REDACTED]
[REDACTED] 167

452. Thus, despite Blackbaud’s claim to the contrary, Blackbaud now admits that it cannot reasonably rely on the promises of cybercriminals that they destroyed the exfiltrated data after Blackbaud paid those cybercriminals a ransom. Even now, because of its insistence on this

¹⁶⁴ *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*, FBI (Oct. 2, 2019), <https://www.ic3.gov/Media/Y2019/PSA191002> [<https://perma.cc/VX8P-TW7F>].

¹⁶⁵ See, e.g., Phil Muncaster, *US Data Breach Volumes Plummet 30% in 2020*, Infosecurity Mag. (Oct. 15, 2020), <https://www.infosecurity-magazine.com/news/us-data-breach-volumes-plummet-30/> [<https://perma.cc/2LYC-XDP6>]; Zack Whittaker, *Decrypted: The Major Ransomware Attack You Probably Didn’t Hear About*, TechCrunch (Oct. 7, 2020), <https://techcrunch.com/2020/10/07/decrypted-blackbaud-ransomware-attack-gets-worse/> [<https://perma.cc/R8M4-FMMC>].

¹⁶⁶ See, e.g., *supra* n.46, 47; Letter from Jeffrey Boogay, att’y at Mullen Coughlin LLC, to Consumer Protection Bureau, Office of the N.H. Att’y Gen. (Aug. 21, 2020), <https://www.doj.nh.gov/consumer/security-breaches/documents/heifer-project-international-20200901.pdf> [<https://perma.cc/TNV9-A4VY>]; Letter from Univ. of Detroit Mercy regarding Notice of Data Breach, <https://oag.ca.gov/system/files/9028629.PDF> (last visited Dec. 18, 2021) [<https://perma.cc/4QU8-SSBY>]. See, e.g., *supra* n.46, 47; Letter from Jeffrey Boogay, att’y at Mullen Coughlin LLC, to Consumer Protection Bureau, Office of the N.H. Att’y Gen. (Aug. 21, 2020), <https://www.doj.nh.gov/consumer/security-breaches/documents/heifer-project-international-20200901.pdf> [<https://perma.cc/TNV9-A4VY>]; Letter from Univ. of Detroit Mercy regarding Notice of Data Breach, <https://oag.ca.gov/system/files/9028629.PDF> (last visited Dec. 18, 2021) [<https://perma.cc/4QU8-SSBY>].

¹⁶⁷ See, e.g., BLKB_MDL_00000001 at 32, 41.

illogical reliance, Blackbaud knowingly and recklessly continues to mislead Plaintiffs and Class members regarding the scope and potential impact of the Data Breach.

453. Despite having knowledge of the attack and compromised stolen data since at least May 2020, Blackbaud willfully and knowingly withheld this knowledge from its affected clients and their constituents who were victims of the fraud until mid-July or August 2020.

454. Blackbaud has obligations and duties created by state and federal law, contracts, industry standards, common law, and representations made to the clients who entrusted Plaintiffs' and others' data to Blackbaud's care to keep Private Information secure, confidential, and protected from unauthorized access and disclosure.

455. Indeed, cyberattacks have become so notorious that, as recently as November 2019, the FBI and the U.S. Secret Service issued warnings to potential targets like Blackbaud, so they are aware of and are prepared for a potential attack.¹⁶⁸

456. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Blackbaud's industry, including by Blackbaud's own admissions in its 2019 Annual Report.¹⁶⁹

457. Blackbaud breached its obligations to Plaintiffs and the Class members, and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard Blackbaud's computer systems and data. Blackbaud's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security program to reduce the risk of data breaches and cyberattacks;

¹⁶⁸ Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), <https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last visited Dec. 19, 2021) (emphasis added) [<https://perma.cc/Z6GF-777F>].

¹⁶⁹ 2019 Form 10-K, *supra* n.8, at 20.

- b. Failing to adequately protect consumers' Private Information;
- c. Failing to properly monitor its own data security programs for existing intrusions;
- d. Failing to destroy highly confidential personal data information including Social Security numbers on its legacy software which was unnecessarily kept on Blackbaud's systems despite no reasonable or practicable business reason for doing so; and
- e. Failing to timely notify its Clients, Plaintiffs, and the Class members of the data breach.

458. As the result of Blackbaud's failure to take certain measures to prevent the attack before it occurred, Blackbaud negligently and unlawfully failed to safeguard Plaintiffs' and Class members' Private Information.

459. Accordingly, as outlined below, Plaintiffs' daily lives were disrupted; Plaintiffs and Class members experienced actual incidents of identity theft and fraud, and Plaintiffs and Class members face an increased risk of fraud and identity theft.

G. Data Breaches Put Consumers at Increased Risk of Fraud and Identity Theft

460. Private Information is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" corporations in America. Illustratively, Alphabet Inc., the parent company of Google, reported in its 2020 Annual Report a total annual revenue of \$182.5 billion and net income of \$40.2 billion.¹⁷⁰ \$160.7 billion of this revenue derived from its Google business, which is driven almost exclusively by leveraging the Private Information it collects about the users of its various free products and services. America's largest corporations profit almost exclusively through the use of Private Information illustrating the considerable market value of personal Private Information.

¹⁷⁰ Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), <https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm>.

461. Criminal law also recognizes the value of Private Information and the serious nature of the theft of such an asset by imposing prison sentences. This strong deterrence is necessary because cybercriminals earn significant revenue through stealing Private Information. Once a cybercriminal has unlawfully acquired personal data, the criminal can demand a ransom or blackmail payment for its destruction, use the information to commit fraud or identity theft, or sell the Private Information to another cybercriminal on a thriving black market.

462. Cybercriminals use “ransomware” to make money and harm victims. Ransomware is a widely known and foreseeable malware threat in which a cybercriminal encrypts a victim’s computer such that the computer’s owner can no longer access any files or use the computer in any way. The cybercriminal then demands a payment for the decryption key. Ransomware is typically propagated through phishing, spear phishing, or visiting a malicious or compromised website that contains a virus or other malware.

463. Once stolen, Private Information can be used in a number of different ways. One of the most common is that it is offered for sale on the “dark web,” a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users’ identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and Private Information. Websites appear and disappear quickly, making it a dynamic environment.

464. The U.S. government, various U.S. and international law enforcement agencies, cybersecurity industry groups and laboratories, and numerous industry trade groups have issued warnings and guidance on managing and mitigating phishing and ransomware threats. There are

industry best practices for cybersecurity related to phishing and ransomware, some of which are particularly effective.

465. For example, in 2019, both Microsoft and Google have publicly reported that using multi-factor authentication (“MFA”) blocks more than 99% of automated hacks, including most ransomware attacks that occur because of unauthorized account access. Likewise, the reputable SANS Software Security Institute issued a paper stating “[t]ime to implement multi-factor authentication!”¹⁷¹ An example of MFA implementation is receiving a text with a code when you input your username and password into a website; even if a cybercriminal knew your username and password, the cybercriminal would not be able to see the code on your phone and would thus be blocked from accessing your online account.

466. In this regard, implementing MFA “can block over 99.9 percent of account compromise attacks.”¹⁷²

467. The FBI concurs, listing “applying two-factor authentication wherever possible” as a best practice to defend against ransomware attacks.¹⁷³

¹⁷¹ Matt Bromiley, *Bye Passwords: New Ways to Authenticate* at 3, SANS Software Security Inst. (July 2019), <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ> [<https://perma.cc/ZSW9-QUEW>]. Matt Bromiley, *Bye Passwords: New Ways to Authenticate* at 3, SANS Software Security Inst. (July 2019), <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ> [<https://perma.cc/ZSW9-QUEW>].

¹⁷² *What Is Multi-Factor Authentication (MFA)?*, Consensus Techs. (Sept. 16, 2020), <https://www.concensus.com/what-is-multi-factor-authentication/#:~:text=The%20proof%20that%20MFA%20works,percent%20of%20account%20compromise%20attacks> [<https://perma.cc/RKT2-LX5Z>].

¹⁷³ *Ransomware Victims Urged to Report Infections to Federal Law Enforcement*, FBI (Sept. 15, 2016), <https://www.ic3.gov/Media/Y2016/PSA160915> [<https://perma.cc/NB42-8ADB>].

468. The industries that Blackbaud serves have seen a substantial increase in cyberattacks and data breaches since as early as 2016.¹⁷⁴

469. Indeed, cyberattacks have become so notorious that the FBI and Secret Service issued a warning in 2019 to potential targets so they were aware of, and prepared for, a potential attack.¹⁷⁵

470. Cyberattacks and data breaches of medical facilities, educational and religious institutions, and non-profit entities are especially problematic because of the disruption they cause to the daily lives of the patients, students, donors, and other individuals affected by attack, including minor children and adults lacking capacity to consent to the disclosure of their information.

471. Perhaps most illustrative of the danger that can be caused by cyberattacks on medical facilities, the first known death from a cyberattack was recently reported in Germany after a ransomware attack crippled a hospital's systems and they were forced to turn away emergency patients.¹⁷⁶

472. The U.S. Government Accountability Office (“GAO”) released a report in 2007 regarding data breaches finding that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”¹⁷⁷

¹⁷⁴ *Id.*

¹⁷⁵ Kochman, *supra* n.171.

¹⁷⁶ Melissa Eddy & Nicole Perlroth, *Cyber Attack Suspected in German Woman’s Death*, N.Y. Times (Sept. 18, 2020), <https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomware-death.html> [<https://perma.cc/VMT8-93B5>].

¹⁷⁷ *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (“GAO Report”) at 2, GAO (June 2007), <https://www.gao.gov/assets/270/262899.pdf> [<https://perma.cc/GCA5-WYA5>].

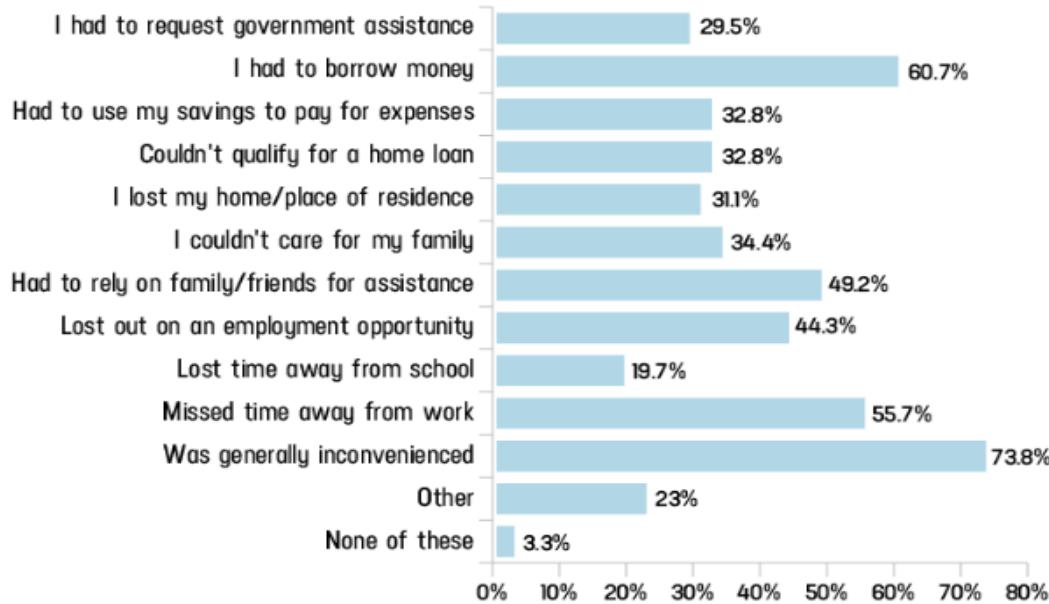
473. The FTC recommends that identity theft victims take several steps to protect their personal health and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.¹⁷⁸

474. Cybercriminals use stolen Private Information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

475. Identity thieves can also use SSNs to obtain a driver's license or other official identification card in the victim's name, but with the thief's picture; use the victim's name and SSN to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, seek unemployment or other benefits, and may even give the victim's Private Information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by the Identity Theft Resource Center ("ITRC") shows the multitude of harms caused by fraudulent use of personal and financial information:

¹⁷⁸ *Identity Theft Recovery Steps*, FTC, <https://www.identitytheft.gov/Steps> (last visited Mar. 23, 2021) [<https://perma.cc/ME45-5N3A>].

Americans' expenses/disruptions as a result of criminal activity in their name [2016]



Source: Identity Theft Resource Center

creditcards.com 179

476. As set forth above, 96.7% of study subjects experienced costs or other harms from the criminal activity.¹⁸⁰ As illustrated in the above graphic, this includes devastating results such as “I lost my home/place of residence” and “I couldn’t care for my family.” Moreover, the harms of identity theft are not limited to the affected individual and may adversely impact other associated persons and support systems, including government assistance programs. In the ITRC study, nearly one third of survey respondents had to request government assistance as a result of the identity theft, such as welfare, EBT, food stamps, or similar support systems.¹⁸¹ The ITRC

¹⁷⁹ Jason Steele, *Credit Card and ID Theft Statistics*, Creditcards.com (updated Oct. 24, 2017), <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> [https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php].

¹⁸⁰ *Id.*

¹⁸¹ *Id.*

study concludes that “identity theft victimization has an extreme and adverse effect on each individual as well as all of the support systems and people associated with the individual.”¹⁸²

477. Private Information is a valuable property right.¹⁸³ Its value is axiomatic, considering the value of Big Data in corporate America as well as the consequences of cyber thefts resulting in heavy prison sentences. This obvious risk to reward analysis illustrates that Private Information has considerable market value that is diminished when it is compromised.

478. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the GAO, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.¹⁸⁴

Private Information is such an inherently valuable commodity to identity thieves that, once it is compromised, criminals often trade the information on the cyber black-market for years.

479. Furthermore, data breaches that expose any personal data, and in particular non-public data of any kind (*e.g.*, donation history or hospital records), directly and materially increase

¹⁸² *Id.*

¹⁸³ See, *e.g.*, John T. Soma et al., *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *1 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”).

¹⁸⁴ GAO Report, *supra* n.177, at 29.

the chance that a potential victim is targeted by a spear phishing attack in the future, and spear phishing results in a high rate of identity theft, fraud, and extortion.¹⁸⁵

480. There is a strong probability that entire batches of stolen information from the Data Breach have yet to be made available on the black market, meaning Plaintiffs and the Class members are at an increased risk of fraud and identity theft for many years into the future. Indeed, some of the Plaintiffs and many of the Class members are in very early stages of their lives—in their twenties and thirties. Thus, as the respective Notices advise, Plaintiffs must vigilantly monitor their financial accounts for many years to come.

H. Blackbaud’s Inadequate Response to the Data Breach

481. After the Data Breach, on May 14, 2020, Blackbaud retained Kudelski Security “investigate unauthorized activity and scripts detected throughout” Blackbaud’s systems.¹⁸⁶ Kudelski completed its analysis on June 10, 2020,¹⁸⁷ and issued the report on July 14, 2020, two days before Blackbaud began contacting customers to inform them that financial information and SSNs might have been stored in unencrypted fields and therefore left exposed.

482. [REDACTED]

[REDACTED]

¹⁸⁵ See Kelion & Tidy, *supra* n.163 (concluding that personal information such as “names, titles, telephone numbers, email addresses, mailing addresses, dates of birth, and, more importantly, donor information such as donation dates, donation amounts, giving capacity, philanthropic interests, and other donor profile information . . . in the hands of fraudsters, [makes consumers] particularly susceptible to spear phishing—a fraudulent email to specific targets while purporting to be a trusted sender, with the aim of convincing victims to hand over information or money or infecting devices with malware”).

¹⁸⁶ Kudelski Security, Blackbaud Incident Report, *supra* n.158.

¹⁸⁷ *Id.*

483. The Kudelski report is incomplete—it does not identify the original point of intrusion—that is *how* the Data Breach began in the first instance. The forensic report does not indicate a root cause of the Data Breach. Nor does the forensic report acknowledge that cybercriminals were able to exploit still-unreported weaknesses in Blackbaud’s environment in order to access and exfiltrate information about Plaintiffs and the Class members. Both Blackbaud and Kudelski stop short—misrepresenting the nature of the Data Breach and failing to pursue the facts to their conclusions, leading to confusion and the false conclusion that Plaintiffs and Class members are not at risk.

484. Upon information and belief, to date, Blackbaud has provided only certain Class members with “Single Credit Bureau Monitoring,” which provides data access to only one of the three national credit reporting bureaus, as well as “access remediation support” from CyberScout Fraud Investigator, for a period of only 24 months from the date of enrollment. This is plainly inadequate, as the compromised Private Information can be utilized by thieves at any time after two years, and as such the threat to Plaintiffs’ and the Class members’ credit or identity will continue for many years thereafter. Beyond this two-year window, Blackbaud offers these victims no assistance or protection, even if identity theft occurs. Consequently, Plaintiffs and Class members have and will incur out of pocket costs including the costs of purchasing credit monitoring services, credit freezes, credit reports, and/or other protective measures to deter, detect, respond to, and address identity theft.

¹⁸⁸ Banda Dep. at 114:19-116:15, 116:19-117:11, 117:25-118:20, 118:22-119:13, 120:10-16, 120:19-21; PX32 at 2-10.

¹⁸⁹ Banda Dep. at 148:21-149:14; PX32 at 12.

485. As a result of the Data Breach, even if Plaintiffs used credit monitoring, the data thieves could wait another seven or more years to sell or use their Private Information without detection. Moreover, cybercriminals may be able to cross-reference information obtained from this Data Breach with other data sources with an astonishingly comprehensive scope and degree of accuracy to build valuable profiles on Plaintiffs and members of the Class. Two years of single-bureau credit monitoring is not enough to protect against these attacks.

486. Further, even if the Class members' credit is frozen, they will eventually need to unfreeze their credit in order to, among other things, obtain any car loans, obtain any mortgages, apply for jobs and various other tasks associated with building and strengthening their credit histories. Doing so will make the Class members vulnerable again in the future.

I. Blackbaud's Inadequate and Misleading Notice

487. Blackbaud has represented that customers' information was never made available on the Dark Web. It was not until July 16, 2020, that Blackbaud publicly disclosed the data breach. Those statements contained several misstatements or omissions:

In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. ... Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted (private cloud) environment. Because protecting our customers' data is our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly.¹⁹⁰

488. Discovery obtained in this case demonstrates that the notice was also misleading.

489. First, Blackbaud had hardly "stopped" a ransomware attack. [REDACTED]

[REDACTED]

¹⁹⁰ *Learn More Announcement*, *supra* n.6 *Learn More Announcement*, *supra* n.6

[REDACTED] 191 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] 192 [REDACTED]

[REDACTED] 193 [REDACTED]

[REDACTED] 194 [REDACTED]

[REDACTED] 195 [REDACTED]

490. [REDACTED]

[REDACTED] 196 [REDACTED]

[REDACTED] 197 [REDACTED]

[REDACTED] 198 [REDACTED]

491. [REDACTED] [REDACTED]

¹⁹¹ Friedberg Dep. at 52:5-9; PX9 at 3 and 4; PX22 at 6.

¹⁹² BLKB_MDL_00000001 at 8, 12-24.

¹⁹³ Friedberg Dep. at 33:6-19; 259:19-24.

¹⁹⁴ Friedberg Dep. at 28:7-29:12.

¹⁹⁵ Friedberg Dep. at 259:16-18; 269:10-18.

¹⁹⁶ BLKB_MDL_00006683 at 1 (noting [REDACTED])

¹⁹⁷ Friedberg Dep. at 279:23-280:2; PX13 at 6 [REDACTED]

¹⁹⁸ Friedberg Dep. at 135:6-22; 138:18--13; 279:23-280:2, 140:4-9, 158:12-160:6; PX14 at 16 [REDACTED]

[REDACTED] 199 [REDACTED]

[REDACTED] 200 [REDACTED]

[REDACTED] 201

492. [REDACTED]

[REDACTED] 202 [REDACTED]

[REDACTED] 203

493. Friedberg admitted [REDACTED]²⁰⁴ Moreover, since the identity of the attacker(s) remains unknown, there is no track record for comparison, and the attacker(s) have no reputation to uphold to abide by their “promise” to delete the information.²⁰⁵

494. Similarly, according to Confidential Witness No. 1, it would be very difficult for Blackbaud to determine if the cybercriminals involved in this case would agree not to release the

¹⁹⁹ PX26 at 2.

²⁰⁰ Friedberg Dep. at 288:18-289:3; PX26 at 1.

²⁰¹ See, e.g., Notice Letters to Class representatives William Glasper (Allina Health), Kassandre Clayton (Trinity Health), William Allen (WakeMed), and Alexandra Mitchell (St. Andrew’s Episcopal School).

²⁰² PX24, at 2.

²⁰³ *Id.* (emphasis added).

²⁰⁴ Friedberg Dep. at 283:15-23.

²⁰⁵ Friedberg Dep. 58:21-59:7; at PX 8 at 16.

stolen Private Information publicly, despite payment of a ransom. “There is no good way to verify that,” Confidential Witness No. 1 says. Further, Confidential Witness No. 1 says that s/he is “bothered” by Blackbaud’s public statement that the cybercriminals destroyed the stolen data. S/he further stated, “[The cybercriminal] is a criminal. You don’t trust him.”

495. Blackbaud’s statements that further misuse or publication of the data is contradicted by its own efforts after the breach to see if the PII of its own executives were posted on the Dark Web.²⁰⁶ [REDACTED]²⁰⁷ [REDACTED]

[REDACTED]²⁰⁸

496. What was stolen has also changed. Blackbaud initially represented to the public, law enforcement, and the Social Good Entities that sensitive information such as Social Security numbers (“SSN”) and bank account numbers were not compromised, in a Form 8-K filing with the SEC on September 29, 2020, Blackbaud buried in its disclosures that this information *was* actually stolen during the “security incident.”²⁰⁹ This was the first time that Blackbaud publicly acknowledged that the information taken in the Data Breach included not only names and addresses, but also that “further forensic investigation found that for some of the notified customers, the cybercriminal may have accessed some unencrypted fields intended for bank account information, [S]ocial [S]ecurity numbers, usernames and/or passwords.”²¹⁰

²⁰⁶ Friedberg Dep. at 276:23-277:15; [REDACTED] BLKB_MDL_00025449.

²⁰⁷ Friedberg Dep. at 277:23-278:3; [REDACTED] BLKB_MDL_00000294.

²⁰⁸ BLKB_MDL_00000294.

²⁰⁹ *Supra* n.46

²¹⁰ *Id.*

VI. PLAINTIFFS' AND CLASS MEMBERS' INJURIES AND DAMAGES

498. Plaintiffs and Class members have been harmed and incurred damages as a result of the compromise of their Private Information in the Data Breach. Plaintiffs' Private Information was compromised as a direct and proximate result of the Data Breach. While the compromise of this information was known as early as May of 2020, Plaintiffs did not receive Notice until July of 2020 at the earliest—*nearly six months after the breach began.*

A. Plaintiffs' and Class Members' Private Information was Compromised in the Data Breach

499. This security incident is not limited to automated attacks against the availability of information in Blackbaud's possession, custody or control. This incident included unauthorized *persons taking possession of the information*, available for their use however and whenever they see fit.

500. Plaintiffs include students and donors to educational institutions, healthcare patients and donors to healthcare organizations, as well as donors to other non-profit organizations—such as international relief funds, museums, charitable trusts, legal rights organizations, animal welfare organizations, child welfare organizations, as well as national and local charities. Plaintiffs were required to provide Private Information that was obtained and maintained by Blackbaud, which Blackbaud had a duty to secure and safeguard.

²¹¹ Friedberg Dep. at 103:16-104:14, 122:11-123:14; PX11 at 13; PX12.

501. Like Plaintiffs, the Class members' Private Information was compromised as a direct and proximate result of the Data Breach.

502. As a direct and proximate result of Blackbaud's conduct, Plaintiffs and the Class members have been damaged because of the disclosure of their Private Information in several ways.

503. First, because Blackbaud paid a ransom to the cybercriminals to avoid disclosure of the data that was already stolen, Blackbaud has already demonstrated to those criminals that the stolen data has value. Accordingly, now Plaintiffs and Class members face their *own* risk of extortion, because there can be no guarantee that the cybercriminals actually deleted the data that they stole.

504. Although Blackbaud will argue that its payment of a ransom diminishes the risk to Plaintiffs and Class members to close to zero, privacy and security professionals disagree, and believe that payment of a ransom may encourage further exploits.

Unlike negotiating for a decryption key, *negotiating for the suppression of stolen data has no finite end*. Once a victim receives a decryption key, it can't be taken away and does not degrade with time. With stolen data, a threat actor can return for a second payment at any point in the future. The track records are too short and evidence that defaults are selectively occurring is already collecting. Accordingly, we strongly advise all victims of data exfiltration to take the hard, but responsible steps. Those include getting the advice of competent privacy attorneys, performing an investigation into what data was taken, and performing the necessary notifications that result from that investigation and counsel. *Paying a threat actor does not discharge any of the above, and given the outcomes that we have recently seen, paying a threat actor not to leak stolen data provides almost no benefit to the victim.*²¹²

²¹² *Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues, supra n.50* (emphasis added).

505. The risk borne by Plaintiffs and Class members is a real one, evidenced by the notices received by the Plaintiffs, which continue to advise Plaintiffs to remain vigilant, monitor their credit, and engage in preventative measures to avoid identity theft.

506. Second, Plaintiffs and Class members have sustained injuries as a result of the disclosure of their Private Information to unauthorized third-party cybercriminals as a result of Blackbaud's insufficient cybersecurity.

507. Plaintiffs have lost the value of their Private Information because the information is a valuable commodity. As discussed herein, Blackbaud demonstrated its value when it paid a ransom to avoid its disclosure. The cybercriminals also recognize its value—placing a price on what it would cost to prevent the disclosure of that information. Further, Blackbaud recognizes the value of the Private Information because it is paid handsomely to protect it.

508. Plaintiffs face real, concrete, and cognizable injuries as a result of the ransomware attack, because cybercriminals confirmed that they exfiltrated data from Blackbaud's systems, and cybersecurity professionals agree that Blackbaud cannot trust the word of criminals in ensuring the safety of Plaintiffs' and Class members' Private Information. The payment of a ransom cannot ensure that the data was deleted, and the Social Good Entities have even warned Plaintiffs and Class members that they must be diligent to prevent identity theft and fraud from occurring as a result of the Data Breach.

509. As a result, Plaintiffs and Class members face immediate and substantial risk of identity theft or fraud, such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

510. Plaintiffs and the Class members also face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as

potential fraudsters could use that information to more effectively target such schemes to Plaintiffs. As a result of Blackbaud's payment of the ransom to the cybercriminals, Blackbaud has also placed Plaintiffs and Class members at risk for being targeted to make ransom payments, themselves, to prevent the disclosure and dissemination of the Private Information that was taken from Blackbaud's systems.

511. Further, Blackbaud has not provided sufficient information to allow Plaintiffs and Class members to adequately protect themselves. As a direct and proximate result of Blackbaud's conduct, Plaintiffs and the Class members have and will continue to incur out-of-pocket costs for protective measures such as on-going credit monitoring fees and may also incur additional costs for credit report fees, and similar costs directly related to the Data Breach.

512. Moreover, Blackbaud's failure to provide complete and accurate information to Plaintiffs, Class members, government officials, and the general public about the Data Breach has prevented Plaintiffs and Class members from obtaining the information they need to mitigate their risk of the future harm described here.

513. Plaintiffs and the Class members have suffered or will suffer actual injury as a direct result of the Data Breach. Plaintiffs and the Class members have and will suffer ascertainable losses in the form of out-of-pocket expenses and/or the loss of the value of their time spent in reasonably acting to remedy or mitigate the effects of the Data Breach relating to:

- a. Finding fraudulent charges;
- b. Canceling and reissuing credit and debit cards;
- c. Addressing their inability to withdraw funds linked to compromised accounts;
- d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- e. Placing "freezes" and "alerts" with credit reporting agencies;

- f. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
- g. Contacting financial institutions and closing or modifying financial accounts;
- h. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;
- i. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled;
- j. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come; and
- k. Interacting with government agencies and law enforcement to address the impact and harm caused by this breach.

514. Further, Plaintiffs and Class members will have to continue to spend significant amounts of time to respond to the Data Breach and monitor their financial, student, and medical accounts and records for misuse.

515. Third, Plaintiffs have, at the very least, sustained nominal damages for Blackbaud's violations as discussed herein. As a result of Blackbaud's failures to safeguard Plaintiffs' and the Class members' Private Information, they are forced to live with the knowledge that their Private Information—which contains private and personal details of their life—may be disclosed to the entire world, thereby making them vulnerable to cybercriminals, permanently subjecting them to loss of security, and depriving Plaintiffs and the Class members of their fundamental right to privacy.

516. Fourth, Plaintiffs are entitled to statutory damages, as provided, based upon the relevant causes of action alleged herein, and described below.

517. Fifth, Blackbaud benefitted at the expense of, and to the detriment of, Plaintiffs and Class members. Among other things, Blackbaud continues to benefit and profit from Class

members' Private Information while its value to Plaintiffs and Class and Subclasses members has been diminished.

518. Finally, Plaintiffs and the Class members have an interest in ensuring that their Private Information, which remains in the possession of Blackbaud, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing Plaintiffs' and the Class members' data is not accessible online and that access to such data is limited and secured.

519. Blackbaud's actions causing the Data Breach, and its failure to provide complete and accurate information to Plaintiffs, Class members, government officials, and the general public about the Data Breach; harms not only Plaintiffs and Class members but also the public interest. Among other things, Blackbaud's failures have prevented government actors from investigating the Data Breach and preventing future harm, and they have eroded the public trust in companies like Blackbaud who are expected to prevent data breaches and be forthcoming about them when they do occur. Thus, injunctive and equitable relief aiming to remedy these issues is in the public interest, and the balance of equities supports such relief.

B. The Private Information of Minors was also Compromised in the Data Breach

520. Plaintiffs include guardians of minor students of educational institutions, who were required to provide Private Information that was obtained and maintained by Blackbaud, which Blackbaud had a duty to secure and safeguard. In some instances, this information included the student's academic records as well as sensitive Private Information.

521. Children's data is particularly attractive to data thieves and can have long-lasting effects on the child's financial history and identity. Specifically:

The theft of a child's identity is lucrative to a cyber-criminal because it can remain undetected for years, if not decades. Without regular monitoring, a child's identity that has been stolen may not be discovered until they are preparing to go to college

and start applying for student loans or get their first credit card. By then, the damage is done and the now young adult will need to go through the pain of proving that their identity was indeed stolen.²¹³

522. In 2011, Carnegie Mellon University’s CyLab reported “the rate of child identity theft is 51 times higher than for adults (whose data sets cost about \$10 - \$25 on dark web markets).”²¹⁴

523. By early 2018, it became well known that the data of infants was being sold on the dark web. As of 2018, the cost of an infant’s data was approximately \$300 in Bitcoin, which would “provide cybercriminals access to a clean credit history.”²¹⁵

524. As instructed by the FTC:

A child’s Social Security number can be used by identity thieves to apply for government benefits, open bank and credit card accounts, apply for a loan or utility service, or rent a place to live.²¹⁶

525. As one cyber-security author further explained, the impact of the use of children’s information is further exacerbated by the fact that there are few checks on using a child’s data to initially obtain credit and slowly increase it over time—all while being undetected by the child and

²¹³ Avery Wolfe, *How Data Breaches Affect Children*, AXIOM Cyber Solutions (Mar. 15, 2018), <https://axiomcyber.com/data-breach/how-data-breaches-affect-children/> [<https://perma.cc/3GAH-2VW4>].

²¹⁴ Selena Larson, *Infant Social Security Numbers Are for Sale on the Dark Web*, CNN Bus. (Jan. 22, 2018), <https://money.cnn.com/2018/01/22/technology/infant-data-dark-web-identity-theft/index.html> [<https://perma.cc/YZ83-6UZ5>].

²¹⁵ *Id.*

²¹⁶ *Consumer Information: Child Identity Theft*, FTC (Sept. 2018), <https://www.consumer.ftc.gov/articles/0040-child-identity-theft> [<https://perma.cc/R46U-8P8D>].

the parents.²¹⁷ Thus, “[t]he problem goes unnoticed for years—possibly decades—before the child goes to apply for student loans, open their first credit card, or buy their first car.”²¹⁸

526. In light of regulations about how children’s Private Information is collected and maintained, the companies providing the service of collecting and maintaining purport to understand this critical concern about the safe keeping of children’s data.

527. Blackbaud has made specific commitments regarding the maintenance of students’ Private Information. In April of 2015, with regard to its K-12 school providers, Blackbaud signed a pledge to respect student data privacy to safeguard student information. The Student Privacy Pledge (the “Pledge”) was created to “safeguard student privacy in the collection, maintenance and use of personal information.”²¹⁹

528. In signing the Pledge, Blackbaud represented to students and parents of its K-12 school providers that it would, (1) “[m]aintain a comprehensive security program;” and (2) “[b]e transparent about collection and use of student data.”²²⁰ Additionally, “[t]he Pledge details ongoing industry practices that meet (and in some cases, exceed) all federal requirements, and encourages service providers to more clearly articulate their data privacy practices.”²²¹

²¹⁷ See Emily Wilson, *The Worrying Trend of Children’s Data Being Sold on the Dark Web*, TNW (Feb. 23, 2019), <https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/> [<https://perma.cc/M7F6-WEC6>].

²¹⁸ *Id.*

²¹⁹ Nicole McGougan, *Blackbaud Signs Pledge to Respect Student Data Privacy*, Blackbaud (Apr. 22, 2015, 1:11 PM), <https://www.blackbaud.com/newsroom/article/2015/04/22/blackbaud-signs-pledge-to-respect-student-data-privacy> (last visited Dec. 19, 2021) [<https://perma.cc/ND22-8Q7K>].

²²⁰ *Id.*

²²¹ *Id.*

529. In further support of this representation and promise to student and parent users, Travis Warrant, president of Blackbaud's K-12 Private Schools Group, stated:

Blackbaud is committed to protecting sensitive student data and security The Pledge will better inform our customers, service providers and the general public of our dedication to protecting student privacy. The Pledge details ongoing industry practices that meet (and in some cases, exceed) all federal requirements, and encourages service providers to more clearly articulate their data privacy practices.²²²

530. Accordingly, the minors have also suffered concrete and particularized injuries as a result of the Data Breach.

C. Plaintiffs' and Class Members' PHI was Compromised in the Data Breach

531. Another group of individuals whose Private Information was compromised in the Data Breach include healthcare patients and donors to healthcare organizations, who were required to provide PHI that was obtained and maintained by Blackbaud, which Blackbaud had a duty to secure and safeguard.

532. Hospital and healthcare provider GPPs must comply with HIPAA and the Health Information Technology for Economic and Clinical Health ("HITECH") Act, including the HHS implementing regulations.

533. A 2013 HIPAA amendment made it easier for HIPAA Covered Entities, such as hospitals and healthcare providers, to target patients for donations by using software solutions like those offered by Blackbaud to enrich electronic Protected Health Information ("ePHI") to maximize outreach to wealthy patients capable of making a meaningful philanthropic gift to the hospital.

²²² *Id.*

534. ePHI is PHI that is produced, saved, transferred, or received in electronic form. PHI is “[i]ndividually identifiable health information . . . received by a health care provider, health plan, employer or healthcare clearing house [and its Business Associates] . . . [that] [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual . . . [t]hat identifies the individual; or [w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.” 45 C.F.R. §§ 160.103, *et seq.*

535. Under the 2013 HIPAA amendments, Covered Entities such as hospitals are permitted to use and disclose ePHI without a written patient authorization for GPPs, including, without limitation, data elements such as the patient’s name, age, gender, date of birth, dates of services, patient’s health insurance status, the department treating the patient (*e.g.*, oncology), the name of the patient’s physician, and the outcome of the patient’s care.

536. Blackbaud provides software solutions to Covered Entities with GPPs.

537. Upon information and belief, Blackbaud’s Covered Entity Clients enter ePHI into Blackbaud hosted solutions for purposes including, but not limited to, analyzing the ePHI in combination with publicly available sources to identify major and principle gift prospects.

538. Blackbaud understood and made representations to the Social Good Entities about both the value and the risk of using ePHI for fundraising purposes. As stated in one of its white papers, Blackbaud understood;

[t]he new HIPAA rules offer great opportunity for hospitals and health systems to reach out in a more meaningful way to the individuals and families who have the greatest affinity to them — their patients. **However, with this opportunity comes**

great responsibility to establish business processes that allow for successful fundraising but also manage and protect the patient data entrusted to you.²²³

539. Covered Entities and their Business Associates, which process PHI and ePHI, must meet strict privacy and security standards propounded by the U.S. Department of Health and Human Services (“HHS”) pursuant to HIPAA and HITECH. HHS’s Office for Civil Rights (“OCR”) is responsible for enforcing the Privacy and Security Rules under HIPAA and HITECH.

540. HIPAA/HITECH mandated security specifications are risk-driven and certain measures must be taken if, after a risk assessment, the specified security measure is determined to be “reasonable and appropriate” in the risk management of the confidentiality, availability, and integrity of ePHI.

541. Encryption of ePHI at rest is a commonly implemented security measure for ePHI stored on systems that can be accessed from the internet (including through a client portal).

542. In fact, HHS mandates that organizations encrypt ePHI in motion and at rest whenever it is “reasonable and appropriate” to do so. If encryption is reasonable and appropriate and an organization fails to implement it, it must document its reasons for not doing so in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.

543. Upon information and belief, Blackbaud is a Business Associate, as that term is defined in HIPAA and HITECH, providing functions that involve the use or disclosure of PHI by Covered Entities.

²²³ Susan U. McLaughlin, et. al, *HIPAA, PHI, and You*, at 4, Blackbaud (Feb. 2015), https://www.blackbaud.com/files/resources/downloads/2015/02.15.HIPAA_GratefulPatient.Whitepaper.pdf (emphasis added) [<https://perma.cc/BP8Z-SNZS>].

544. In fact, several notices regarding the Data Breach identify Blackbaud as a “Business Associate.”

545. As a Business Associate, Blackbaud is directly subject to the HIPAA Security Rule.

546. As a Business Associate, Blackbaud is directly liable for HIPAA violations for any “failure to comply with the requirements of the Security Rule.”

547. As a Business Associate, Blackbaud is also directly liable for HIPAA violations for any “failure to provide breach notification to a covered entity or another business associate.”

548. The HIPAA Breach Notification Rule, 45 C.F.R. § 164.400-414, requires HIPAA Covered Entities and their Business Associates to provide notification following a breach of unsecured PHI. Similar breach notification provisions implemented and enforced by the FTC, apply to vendors of personal health records and their third-party service providers, pursuant to Section 13407 of the HITECH Act.

549. A HIPAA breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- b. The unauthorized person who used the PHI or to whom the disclosure was made;
- c. Whether the PHI was actually acquired or viewed; and
- d. The extent to which the risk to the PHI has been mitigated.

550. HHS's OCR issued a "Fact Sheet" on "Ransomware and HIPAA."²²⁴ Where there is an unauthorized disclosure or ransomware attack on PHI the Business Associate must document by "thorough and accurate evaluation the evidence acquired and analyzed" to determine whether there is a "low probability of compromise."²²⁵

551. Blackbaud was aware of the significant privacy and security obligations of Covered Entities and their Business Associates mandated by HIPAA and HITECH and the Privacy and Security Rules.

552. In fact, Blackbaud publishes a white paper on its website describing HIPAA privacy and security issues inherent in the collection and disclosure of PHI for fundraising purposes.²²⁶

553. Based on the Notices issued by Blackbaud's Covered Entity Clients to their patients, Entities that were using Blackbaud software to enrich ePHI were impacted by the Data Breach.

554. Blackbaud's Covered Entity Clients notified their patients of likely unauthorized exposure of PHI stored by Blackbaud on its servers in an unencrypted manner.

555. Blackbaud also designs products for GPPs, which use applications including but not limited to Blackbaud's Research Point software tool. GPPs are fundraising activities conducted in support of nonprofit hospitals and healthcare providers that allow hospitals to identify major philanthropic gift prospects from their patient populations. As described by *The New York Times*, in furtherance of GPPs:

²²⁴ FACT SHEET: Ransomware and HIPAA, HHS Office of Civil Rights, <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf> (last visited Dec. 19, 2021) [<https://perma.cc/VF5Z-RCVM>].

²²⁵ *Id.* at 6.

²²⁶ *Supra* n.223.

Many hospitals conduct nightly wealth screenings [of hospital patients] — using software that culls public data such as property records, contributions to political campaigns and other charities — to gauge which patients are most likely to be the source of large donations. Those who seem promising targets for fund-raising may receive a visit from a hospital executive in their rooms, as well as extra amenities like a bathrobe or a nicer waiting area for their families.²²⁷

556. Through Blackbaud's GPP, hospitals and healthcare systems collect and utilize medical information such as patient numbers, dates of treatment(s), departments of treatment(s), room numbers, health insurance status, and other data that may easily reveal medical diagnosis and related PHI (*e.g.*, being treated by the oncology department would reveal the patient was treated for a cancer diagnosis). This information is collected—without authorization from the patient—and analyzed to determine what kind of donation a former patient would likely make.

557. Accordingly, Plaintiffs and Class members whose PHI was compromised in the Data Breach sustained additional injuries, including statutory damages related to the exposure of their PHI.

VII. CLASS ACTION ALLEGATIONS

558. Plaintiffs bring this action on their own behalf and on behalf of all natural persons similarly situated, as referred to throughout this Complaint as “Class members.”

559. Pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3), and (c)(4) as applicable, Plaintiffs propose the following Nationwide Class and Subclass definitions, subject to amendment as appropriate:

Nationwide Class: All natural persons residing in the United States whose Personally Identifiable Information and/or Protected Health Information was compromised as a result of the Data Breach.

²²⁷ Phil Galewitz, *Hospitals Are Asking Their Own Patients to Donate Money*, N. Y. Times (Jan. 24, 2019), <https://www.nytimes.com/2019/01/24/business/hospitals-asking-patients-donate-money.html> [<https://perma.cc/A25F-W78Z>].

560. Pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiffs propose the following state-by-state claims in the alternative to the nationwide claims, as well as statutory claims brought under state data breach and consumer protection statutes, on behalf of statewide subclasses for each State, the District of Columbia, Puerto Rico, and the Virgin Islands (the “Statewide Subclasses”), subject to amendment as appropriate:

[State] Subclass: All natural persons residing in [name of state or territory] whose Personally Identifiable Information and/or Protected Health Information was compromised as a result of the Data Breach.

561. Excluded from the Class and Subclasses are Blackbaud’s officers, directors, and employees; any entity in which Blackbaud has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Blackbaud. Excluded also from the Class and Subclasses are members of the judiciary to whom this case is assigned, their families and members of their staff.

562. **Numerosity under Federal Rule of Civil Procedure 23(a)(1).** The members of the Class (and Subclasses) are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While the exact number of Class members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of millions of persons whose data was compromised in the Data Breach, who can be identified by reviewing the Private Information exfiltrated from Blackbaud’s databases.

563. **Commonality under Federal Rule of Civil Procedure 23(a)(2).** There are questions of law and fact common to Plaintiffs and Class members, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

- a. Whether Blackbaud unlawfully used, maintained, lost, or disclosed Plaintiffs’ and the Class members’ Private Information;

- b. Whether Blackbaud failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- c. Whether Blackbaud truthfully represented the nature of its security systems, including their vulnerability to hackers;
- d. Whether Blackbaud's data security programs prior to and during the Data Breach complied with applicable data security laws and regulations;
- e. Whether Blackbaud's data security programs prior to and during the Data Breach were consistent with industry standards;
- f. Whether Blackbaud owed a duty to Class members to safeguard their Private Information;
- g. Whether Blackbaud breached its duty to Class members to safeguard their Private Information;
- h. Whether cyberhackers obtained, sold, copied, stored or released Class members' Private Information;
- i. Whether Blackbaud knew or should have known that its data security programs and monitoring processes were deficient;
- j. Whether the Class members suffered legally cognizable damages as a result of Blackbaud's misconduct;
- k. Whether Blackbaud's conduct was negligent;
- l. Whether Blackbaud's conduct was negligent *per se*;
- m. Whether Blackbaud's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;
- n. Whether Blackbaud failed to provide accurate and complete notice of the Data Breach in a timely manner; and
- o. Whether the Class members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

564. **Typicality under Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of those of the Class members because Plaintiffs' Private Information, like that of every Class member, was compromised in the Data Breach.

565. **Adequacy of Representation under Federal Rule of Civil Procedure (a)(4).**

Plaintiffs will fairly and adequately represent and protect the interests of Class members, including those from states and jurisdictions where they may not reside. Plaintiffs' Counsel are competent

and experienced in litigating class actions and were appointed to lead this litigation by the Court pursuant to Federal Rule of Civil Procedure 23(g).

566. **Predominance under Federal Rule of Civil Procedure 23(b)(3).** Blackbaud has engaged in a common course of conduct toward Plaintiffs and the Class members, in that all Plaintiffs' and the Class members' data at issue here was stored by Blackbaud and accessed during the Data Breach. The common issues arising from Blackbaud's conduct affecting Class members, as described *supra*, predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

567. **Superiority under Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class members would find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Blackbaud. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

568. **Injunctive Relief is Appropriate under Federal Rule of Civil Procedure 23(b)(2).** Blackbaud has failed to take actions to safeguard Plaintiffs' and Class members' Private Information such that injunctive relief is appropriate and necessary. Blackbaud has acted on grounds that apply generally to the Class (and Subclasses) as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

Blackbaud has also failed to provide Class members with accurate information concerning the ransomware attack in its disclosures to Class members sufficient to allow them to protect themselves through mitigation efforts or other diligence.

569. Issue Certification Appropriate under Federal Rule of Civil Procedure

23(c)(4). In the alternative, this litigation can be brought and maintained a class action with respect to particular issues, such as Blackbaud's liability with respect to the foregoing causes of action.

VIII. CAUSES OF ACTION

570. Plaintiffs bring these causes of action on behalf of the Nationwide Class and Subclasses, as defined herein. The application of South Carolina law is appropriate because the data breach occurred in South Carolina.

571. Many of Blackbaud's top security decision-makers were based in Blackbaud's South Carolina Office before, during and after the data breach, including Blackbaud's CISO, Rich Friedberg²²⁸; Executive Vice President and Chief Product Officer, Kevin McDearis,²²⁹ Deputy CISO, Ryan Hammer;²³⁰ Senior Director, Risk and Compliance, Ryan Roberts,²³¹ as were additional security team members such as John Underwood²³² and Cyber Security Governance Team Lead, Ashley Wyand;²³³ and also high executive officers including CEO and President, Mike Gianoni.²³⁴

²²⁸ See PX7 (Rich Friedberg's LinkedIn profile); Friedberg Dep. at 61:9-20; BLKB_MDL_00000294.

²²⁹ See BLKB_MDL_00001283.

²³⁰ See PX 23 at 7; BLKB_MDL_00068691.

²³¹ See BLKB_MDL_00068691.

²³² See BLKB_MDL_00126594.

²³³ See BLKB_MDL_00054247 and BLKB_MDL_00025315.

²³⁴ See BLKB_MDL_00175494.

572. During the data breach and its subsequent investigation, Blackbaud’s Chief Information Security Officer, Rich Friedberg was based in Charleston, South Carolina.²³⁵ Mr. Friedberg testified, [REDACTED]

[REDACTED]²³⁶ On September 23, 2020, Mr. Friedberg advised [REDACTED]

[REDACTED]²³⁷

573. Blackbaud’s former Security Operations Center lead, Dale Leonard, testified Blackbaud hosted a “security summit twice a year,” “where we would bring the entire cybersecurity org either into Charleston or into Austin,” where Blackbaud’s cybersecurity team would “do incident-handling procedures, such that if we had a major incident, how the incident would be handled,” and those meetings would also be attended by Blackbaud’s cyberengineering team, HR, legal, and corporation communications, “so on and so forth, so that we could literally test an end-to-end incident handling.”²³⁸

574. According to Mr. Leonard, Blackbaud’s cybersecurity team, mainly the operations and threat groups, maintained [REDACTED]

[REDACTED]²³⁹ [REDACTED]

²³⁵ PX7 (Rich Friedberg’s LinkedIn profile).

²³⁶ Friedberg Dep. at 61:9-20.

²³⁷ See BLKB_MDL_00000294.

²³⁸ See BLKB_MDL_00001283.

²³⁹ See *id.*

575. After the breach was underway, on February 19, 2020, James Underwood, Security Architect, Principal, Cyber Security Architecture & Engagement, based in Charleston, South Carolina, requested Ricky Banda, Blackbaud's Principal Security Engineer, Threat Detection & Response, help Mr. Underwood supply Blackbaud's Corporate IT department with an assessment of an earlier incident, [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED] ²⁴¹ Mr. Underwood thanked Mr. Banda for his assessment regarding a [REDACTED]

576. Blackbaud's President & CEO, Mike Gianoni, and Blackbaud's Vice President Corporate Marketing, Amy Lucia, were both based in Charleston, South Carolina when reviewing responses to Blackbaud's customers in relation to the data breach on August 19, 2020.²⁴³

²⁴⁰ Leonard Dep. at 87:15-88:8.

²⁴¹ *Id.* at 80:3-16.

²⁴² *Id.* at 106:10-107:5.

²⁴³ See BLKB_MDL_00126594.

577. Blackbaud's internal employee communications and external customer communications relating to security incidents and the data breach were drafted by South Carolina based executives including Vice President Corporate Marketing, Amy Lucia,²⁴⁴ and by Sr. Marketing Communications Manager, Corporate Marketing, Cuthbert Langley.²⁴⁵ [REDACTED]

[REDACTED] 246

578. On May 7, 2020, Blackbaud's Sr. Marketing Communications Manager, Corporate Marketing, Cuthbert Langley, based in Charleston South Carolina, "drafted an internal notification regarding the security incident," and Ms. Wyand thought Ms. Langley's updates to the message were appropriate and offered that if customers did reach out with questions regarding "general security/etc. here at Blackbaud," her Cybersecurity governance group could "send them any white papers or extra collateral as needed."²⁴⁷

579. [REDACTED]

[REDACTED]
[REDACTED] 248
[REDACTED]

580. On June 8, 2020, Mr. Hammer requested "a status report on the last of the deliverables," from Darrell Switzer, Director – Global Incident Response Services, Kudelski Security, Inc., and learned that [REDACTED]

²⁴⁴ See *id.*

²⁴⁵ See BLKB_MDL_00025315.

²⁴⁶ Friedberg Dep. at 61:9-20.

²⁴⁷ See BLKB_MDL_00126594.

²⁴⁸ See BLKB_MDL_00175494.

[REDACTED]
[REDACTED] 249

581. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] 250

582. Dale Leonard, Blackbaud's former Security Operations Lead, testified [REDACTED]

[REDACTED] 251

583. Mr. Leonard further testified Blackbaud's cybersecurity team held twice-annual Cybersecurity "Summits," often located in South Carolina which were attended by the entire cybersecurity staff in addition to representatives from other Blackbaud business units in order to test cyber security incident handling.²⁵²

²⁴⁹ See BLKB_MDL_00054247.

²⁵⁰ See BLKB_MDL_00025315.

²⁵¹ Leonard Dep. at 80:3-16, 106:10-107:5.

²⁵² *Id.* at 87:15-88:8.

584. Blackbaud signed a Service Agreement and two Statements of Work with GroupSense for Incident Response and Threat Actor Negotiations, noting Blackbaud was a Delaware corporation with offices in South Carolina.²⁵³

585. Blackbaud's Sr. Vice President and General Counsel Jon Olson signed a Services Agreement and two statements of work, [REDACTED]

[REDACTED] to "Blackbaud, Inc., a Delaware corporation with offices at 2000 Daniel Island Drive, Charleston, SC 29492 ('Blackbaud')."²⁵⁴

586. Plaintiffs allege claims under the laws of individuals in all 50 states and territories because, based upon information and belief and the reasonable investigation of counsel given the limited information made available by Blackbaud concerning the Data Breach, individuals from all jurisdictions suffered injuries as a direct and proximate result of the Data Breach. Plaintiffs have standing to represent individuals in every jurisdiction, as described herein. To force Plaintiffs to search for specific, named representatives for all states at this stage in the litigation serves no useful purpose. *See, e.g., In re Equifax, Inc., Customer Data Security Breach Litig.*, 362 F. Supp. 3d 1295, 1344 (N.D. Ga. 2019); *In re Target Corp. Data Security Breach Litig.*, 66 F. Supp. 3d 1154, 1160 (D. Minn. 2014).

²⁵³ See BLKB_MDL_00008770.

²⁵⁴ See PX 23 at 7.

A. CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1: NEGLIGENCE

On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of Plaintiffs and the Subclasses

587. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

588. The Social Good Entities required Plaintiffs, Class and Subclass members to submit non-public, personal information in order to make charitable contributions to non-profit organizations, and/or obtain medical, educational, and other services.

589. In providing their Private Information, Plaintiffs, Class and Subclass members had a reasonable expectation that this information would be securely maintained and not easily accessible to, or exfiltrated by cybercriminals.

590. Further, Plaintiffs, Class and Subclasses members had a reasonable expectation that in the event of a data breach, Blackbaud would provide timely and adequate notice to the Social Good Entities and/or to them, and would properly identify what Private Information was exposed during a data breach so that Plaintiffs, Class and Subclass members could take prompt and appropriate steps to safeguard their identities.

591. Blackbaud, as an entity that collects sensitive, private data from consumers such as Plaintiffs, Class and Subclass members, and likewise stores and maintains that data, has a duty arising independently from any contract to protect that information.

592. Specifically, Blackbaud, as the purported expert guardian and gatekeeper of data, had a duty to Plaintiffs, Class and Subclass members to securely maintain the Private Information collected as promised, warranted, and in a reasonable manner which would prevent cybercriminals from accessing and exfiltrating this information.

593. By undertaking the duty to maintain and secure this data, sharing it and using it for commercial gain, Blackbaud had a duty of care to use reasonable means to secure and safeguard

its systems and networks—and Plaintiffs, Class and Subclass members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from cyber theft.

594. Blackbaud's duty included a responsibility to implement systems and processes by which it could detect and prevent a breach of its security systems in an expeditious manner and to give prompt and adequate notice to those affected by a data breach and/or ransomware attack.

595. Blackbaud owed a duty of care to Plaintiffs, Class and Subclass members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected and safeguarded the Private Information of the Plaintiffs, Class and Subclasses.

596. Blackbaud's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Blackbaud and Plaintiffs, Class and Subclass members, the end users of the services Blackbaud provided to its clients. While this special relationship exists independent from any contract, it is recognized by Blackbaud's Privacy Policy, as well as applicable laws and regulations. Specifically, Blackbaud actively solicited Private Information as part of its business and was solely responsible for and in the position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs, Class and Subclass members from a resulting data breach.

597. Likewise, as the guardian and gatekeeper of Plaintiffs, Class and Subclass members' Private Information, a special duty existed between Blackbaud and Plaintiffs, Class and Subclass members to promptly and adequately provide notice of the data breach and/or ransomware in a manner that would allow Plaintiffs, Class and Subclass members to take prompt and appropriate steps to safeguard their identities.

598. Blackbaud also had a common law duty to prevent foreseeable harm to others. Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices. It was foreseeable that Plaintiffs and Class members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

599. Blackbaud knew or should have known that the Plaintiffs, Class and Subclass members were relying on Blackbaud to adequately safeguard and maintain their Private Information.

600. In fact, Blackbaud publicly acknowledged Plaintiffs, Class and Subclass members' reliance on Blackbaud's duty to safeguard their Private Information in its 2019 Annual Report, Blackbaud directly addressed its myriad security obligations as well as its known susceptibility to cyberattacks. Specifically, the report states:

If the security of our software is breached, we fail to securely collect, store and transmit customer information, or we fail to safeguard confidential donor data, we could be exposed to liability, litigation, penalties and remedial costs and our reputation and business could suffer. [Emphasis Added]

601. Although Blackbaud management had been repeatedly notified by employees that the systems and networks at issue in this data breach and/or ransomware were vulnerable, not secure, and that a cybercriminal attack may be successful, Blackbaud ignored the warnings and failed to improve its data safeguards and secure Plaintiffs, Class and Subclass members' Private Information.

602. Rich Friedberg, the recent former "CISO" for Blackbaud admitted [REDACTED]

[REDACTED] ²⁵⁵ He

²⁵⁵ Friedberg Dep. at 45:2-5, 46:16-24, 212:5-17, 213:2-12; PX19 at 1, 5.

acknowledged Blackbaud [REDACTED] in
August of 2016²⁵⁶ and that [REDACTED]
[REDACTED] in 2019.²⁵⁷

603. Further, after discovering that cybercriminals had infiltrated its systems and networks, Blackbaud failed to timely notify the Social Good Entities or perform a proper forensic analysis of what data had been exposed, consequently, causing notice to Plaintiffs, Class, and Subclass members to be untimely and insufficient to identify what Private Information had been exposed. [REDACTED]

[REDACTED] 258 [REDACTED] 259

[REDACTED] 260 [REDACTED]

[REDACTED] 261

²⁵⁶ Friedberg Dep. at 44:4-19, 179:12-24, 191:21-25; PX17 at 12, 13, 18.

²⁵⁷ Friedberg Dep. 192:1-9; PX11 at 10-11.

²⁵⁸ *Supra* n.7

²⁵⁹ *Supra* n.8

²⁶⁰ Friedberg Dep. at 259:16-18, 261:18-262:12; 268:19-22; 269:10-18; PX22 at 6.

²⁶¹ Friedberg Dep. at 283:15-23; PX 288:18-289:3; PX24 at 2; PX26 at 1.

604. Blackbaud had additional duties to safeguard Plaintiffs, Class and Subclass members' data through federal and state regulations, including the FTC Act and state consumer protection statutes.²⁶²

605. Blackbaud's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Blackbaud is bound by industry standards to protect confidential Private Information.

606. Blackbaud breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Plaintiffs, Class and Subclass members' data. The specific negligent acts and omissions committed by Blackbaud include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs, Class and Subclass members' Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to and exfiltration of Plaintiffs, Class, Subclass members' Private Information;
- e. Failing to timely detect that Plaintiffs, Class and Subclass members' Private Information had been compromised;
- f. Failing to perform a proper initial forensic investigation that identified what Personal Information had been compromised, resulting in inaccurate notices provided to the Social Good Entities and consequently to Plaintiffs, Class and Subclass members;
- g. Failing to provide timely notice that Plaintiffs, Class and Subclass members' Private Information had been compromised so those at risk could take timely and appropriate steps to mitigate the potential for identity theft and other damages; and
- h. Failing to provide adequate notice of what Private Information had been compromised so that Plaintiffs, Class and Subclass members at risk could

²⁶² See Under COPPA, data deletion isn't just a good idea. It's the law. FTC, (May 31, 2018), <https://www.ftc.gov/news-events/blogs/business-blog/2018/05/under-coppa-data-deletion-isnt-just-good-idea-its-law> [<https://perma.cc/JWT2-KK3L>].

take timely and appropriate steps to mitigate the potential for identify theft and other damages.

607. It was foreseeable to Blackbaud that its failure to use reasonable measures to protect Plaintiffs, Class and Subclasses members' Private Information, including when it warned its systems and networks were vulnerable to cyberattack, would result in injury to Plaintiffs, Class and Subclass members. Further, the breach of security was reasonably foreseeable given the known high frequency of ransomware attacks and data breaches.

608. It was additionally foreseeable to Blackbaud that failure to timely and adequately provide notice of the Data Breach would result in Plaintiffs, Class and Subclass members not being afforded the ability to timely safeguard their identities.

609. It was therefore foreseeable to Blackbaud that its failure to adequately safeguard Plaintiffs, Class and Subclass members' Private Information or provide timely and adequate notice of the Data Breach, would result in one or more types of injuries to Plaintiffs, Class and Subclasses members.

610. Plaintiffs are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

611. Plaintiffs are also entitled to injunctive relief requiring Blackbaud to, *e.g.*, (i) strengthen its data security programs and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; (iii) immediately provide robust and adequate credit monitoring to all Class members; and (iv) correct its past inaccurate and incomplete statements to Plaintiffs, Class members, government officials, and the general public about the Data Breach, and any other relief this Court deems just and proper.

COUNT 2: GROSS NEGLIGENCE
On behalf of Plaintiffs and the Nationwide Class,
or alternatively, on behalf of Plaintiffs and the Subclasses

612. Plaintiffs repeat and reallege all preceding paragraphs, including those from Count I, as if fully alleged herein.

613. Plaintiffs were required to submit non-public Private Information in order to make charitable contributions to the Social Good Entities, and/or obtain medical, educational, and other services. Blackbaud had a duty to Plaintiffs to securely maintain the Private Information collected as promised and warranted.

614. However, Blackbaud maintained unencrypted Personal Information on certain programs. Blackbaud also maintained outdated, legacy versions of its Educational Edge and other programs which were no longer in active use.

615. Blackbaud knew this information was (a) unencrypted and thus subject to breach and misuse; (b) could not be seen by the Social Good Entities; (c) included highly sensitive Private Information; and (d) was “at rest,” meaning the data was not in transit and being actively used.

616. The failure to encrypt this “at rest” obsolete data containing highly sensitive Personal Information on legacy and/or back-up versions of Blackbaud systems was particularly flagrant and egregious. Indeed, this unencrypted Private Information on legacy and/or back-up versions made public exposure of this Private Information in a cyberattack very likely.

617. Moreover, there was no reasonable reason for retaining these records which contain highly sensitive Private Information, including SSNs. Blackbaud has, in fact, acknowledged its failure to encrypt this highly sensitive Private Information.

618. Thus, despite Blackbaud’s initial representations that no sensitive Personal Information was accessed, the highly sensitive, *unencrypted* Personal Information of Plaintiffs was accessed, exfiltrated and otherwise exposed by the Data Breach.

619. By voluntarily accepting the duty to maintain and secure this data, and sharing it and using it for commercial gain, Blackbaud had a duty of care to use reasonable means to secure and safeguard its computer systems to prevent disclosure of the information, and to safeguard the information from cyber theft.

620. Blackbaud's duty included a responsibility to implement systems and processes by which it could detect and prevent a breach of its security systems in an expeditious manner and to give prompt notice to those affected by a data breach and/or ransomware attack.

621. Blackbaud owed a duty of care to Plaintiffs to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected and safeguarded Plaintiffs' Private Information.

622. Blackbaud owed an additional duty to Plaintiffs to take measures to ensure that, *inter alia*:

- a. all Private Information was encrypted and continued to be encrypted;
- b. "at rest" data is deleted after a reasonable amount of time; and/or
- c. Social Good Entities and Plaintiffs were notified that their "at rest," sensitive and unencrypted Private Information had continued to be stored.

623. Blackbaud's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Blackbaud and Plaintiffs, the end users of the services Blackbaud provided to its clients, which is recognized by Blackbaud's Privacy Policy, as well as applicable laws and regulations. Blackbaud actively solicited Private Information as part of its business and was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs from a ransomware attack and resulting data breach.

624. Pursuant to the FTC Act, 15 U.S.C. § 45, Blackbaud had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and the Class

members' Private Information. Plaintiffs and the Class members are the individuals whom the FTC Act is intended to protect.

625. Pursuant to HIPAA, 42 U.S.C. § 1320d, Blackbaud had a duty to securely store and maintain Plaintiffs' and the Class members' Private Information. Plaintiffs and the Class members are the individuals whom HIPAA is intended to protect.

626. Pursuant to the COPPA, 15 U.S.C. §§ 6501-6505, Blackbaud had a duty to: (i) get parental consent before collecting personal information from children under 13; (ii) provide parents with the right to review and delete their children's information; and (iii) could only retain children's personal information for only as long as is reasonably necessary to fulfill the purpose for which the information was collected, and thereafter had a duty to delete any and all child's personal information using reasonable measures to ensure it's been securely destroyed, even absent a parent's request for the deletion of a child's personal information. Minor Plaintiffs and minor Class members are the individuals whom COPPA is intended to protect.

627. Blackbaud's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Blackbaud is bound by industry standards to protect confidential Private Information.

628. Blackbaud consciously failed to use reasonable measures to protect Plaintiffs and Class members' data. The specific gross negligent acts and omissions committed by Blackbaud include, but are not limited to, the following:

- a. Consciously failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs and Class members' Private Information;
- b. Consciously failing to ensure all sensitive Personal Information was encrypted;
- c. Consciously failing to ensure all "at rest" data was destroyed in a reasonable amount of time;

- d. Consciously failing to notify the Social Good Entities, Plaintiffs, and Class members that unencrypted, “at rest” data was still maintained by Blackbaud;
- e. Consciously failing to adequately monitor the security of its networks and systems;
- f. Consciously failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;
- g. Consciously allowing unauthorized access to Class members’ Private Information;
- h. Consciously failing to detect in a timely manner that Class members’ Private Information had been compromised; and
- i. Consciously failing to timely notify Plaintiffs and Class members about the Data Breach so those put at risk could take timely and appropriate steps to mitigate the potential for identity theft and other damages.

629. It was foreseeable that Blackbaud’s conscious failure to use reasonable measures to protect the Plaintiffs’ and Class members’ Private Information would result in injury to the Plaintiffs and Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of ransomware attacks and data breaches.

630. It was therefore foreseeable that the conscious failure to adequately safeguard the Plaintiffs’ and Class members’ Private Information would result in one or more types of injuries to Plaintiffs and Class members.

631. Blackbaud paid a ransom to ensure that cybercriminals did not publish Plaintiffs’ and Class members’ data. As a result, cybercriminals now know that the Private Information of Plaintiffs and Class members is valuable enough to fetch a ransom. It is thus foreseeable that, in making a ransom payment, Blackbaud is subjecting Plaintiffs and Class members to further targeting by cybercriminals’ further demands for ransom from the Plaintiffs and Class members, as well as identity theft and fraud.

632. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

633. Plaintiffs and Class members are also entitled to injunctive relief requiring Blackbaud to, *e.g.*, (i) identify all legacy data it still maintains; (ii) destroy or encrypt legacy data that has been “at rest” for an unreasonable amount of time; (iii) notify all Social Good Entities and consumers with legacy data that is still be maintained by Blackbaud; (iv) strengthen its data security programs and monitoring procedures; (v) submit to future annual audits of those systems and monitoring procedures; (vi) immediately provide robust and adequate credit monitoring to Plaintiffs and Legacy/Back-up Subclass members; and (iv) correct its past inaccurate and incomplete statements to Plaintiffs, Class members, government officials, and the general public about the Data Breach, and any other relief this Court deems just and proper.

COUNT 3: DECLARATORY JUDGMENT
On behalf of Plaintiffs and the Nationwide Class,
or alternatively, on behalf of Plaintiffs and the Subclasses

634. Plaintiffs repeat and allege all preceding paragraphs, as if fully alleged herein.

635. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

636. An actual controversy has arisen in the wake of the Data Breach regarding its present and prospective common law and other duties to reasonably safeguard Plaintiffs, Class and Subclass members’ Private Information and whether Blackbaud is currently maintaining data security measures adequate to protect Plaintiffs, the Class and Subclasses members from further, future data breaches that compromise their Private Information.

637. Plaintiffs, Class and Subclass members allege that Blackbaud’s data security measures remain inadequate and Blackbaud has not provided any evidence that it has remedied

the failure that occurred in the Data Breach at issue or has remedied any other vulnerability from its failure to properly assess threats by cybercriminals.

638. Plaintiffs, the Class and Subclass members continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

639. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Blackbaud continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, the FTC Act, HIPAA, COPPA, and various state statutes;
- b. Blackbaud owes a duty by virtue of its special relationship, understanding that it is safeguarding sensitive, Private Information, or that it has already acknowledged a responsibility to keep such information safe by virtue of security policies; and
- c. Blackbaud continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

640. The Court also should issue corresponding prospective injunctive relief requiring Blackbaud to, *e.g.*, (i) identify all legacy data it still maintains; (ii) destroy or encrypt legacy data that has been "at rest" for an unreasonable amount of time; (iii) notify all Social Good Entities and consumers with legacy data that is still be maintained by Blackbaud; (iv) strengthen its data security programs and monitoring procedures; (v) submit to future annual audits of those systems and monitoring procedures; (vi) immediately provide robust and adequate credit monitoring to Plaintiffs and Legacy/Back-up Subclass members; and (iv) correct its past inaccurate and incomplete statements to Plaintiffs, Class members, government officials, and the general public about the Data Breach, and any other relief this Court deems just and proper. Class members lack the knowledge and information necessary to take adequate measures to protect themselves, and

have been quelled into a false sense of security based upon Blackbaud's misrepresentations and omissions in its publicly-facing statements.

641. If an injunction is not issued, Plaintiffs, the Class and Subclass members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Blackbaud. The risk of another such breach is real, immediate, and substantial. If another breach at Blackbaud occurs, Plaintiffs, the Class and Subclass members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

642. The hardship to Plaintiffs, the Class and Subclass members if an injunction does not issue exceeds the hardship to Blackbaud if an injunction is issued. Among other things, if another massive data breach occurs at Blackbaud, Plaintiffs, the Class and Subclass members will likely be subjected to substantial identify theft and other damage (as they cannot elect to store their information with another company). On the other hand, the cost to Blackbaud of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Blackbaud has a pre-existing legal obligation to employ such measures.

643. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by helping to prevent another data breach at Blackbaud, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose Private Information would be further compromised.

COUNT 4: INVASION OF PRIVACY
On behalf of Plaintiffs and the Nationwide Class,
or alternatively, on behalf of Plaintiffs and the Subclasses

644. Plaintiffs repeat and reallege all preceding paragraphs, as if fully alleged herein.

645. Plaintiffs, Class and Subclass members have a legally protected privacy interest in their Private Information, which is and was collected, stored and maintained by Blackbaud, and

they are entitled to the reasonable and adequate protection of their Private Information against foreseeable unauthorized access, as occurred with the Data Breach.

646. Plaintiffs, Class and Subclass members reasonably expected that Blackbaud would protect and secure their Private Information from unauthorized parties and that their Private Information would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

647. Blackbaud unlawfully invaded the privacy rights of Plaintiffs, Class and Subclasses members by engaging in the conduct described above, including by failing to protect their Private Information by permitting unauthorized third-parties to access, exfiltrate and view this Private Information. Likewise, Blackbaud further invaded the privacy rights of Plaintiffs, Class and Subclass members, and permitted cybercriminals to invade the privacy rights of Plaintiffs, Class and Subclass members, by unreasonably and intentionally delaying disclosure of the Data Breach, and failing to properly identify what Private Information had been accessed, exfiltrated, and viewed by unauthorized third-parties.

648. This invasion of privacy resulted from Blackbaud's failure to properly secure and maintain Plaintiffs, the Class and Subclasses members' Private Information, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

649. Plaintiffs, the Class and Subclasses members' Private Information is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs, the Class and Subclasses members' Private Information, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

650. The disclosure of Plaintiffs, the Class and Subclasses members' Private Information to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

651. Blackbaud's willful and reckless conduct which permitted unauthorized access, exfiltration and disclosure of Plaintiffs' and the Class and Subclasses members' sensitive, Private Information is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

652. The unauthorized access, exfiltration, and disclosure of Plaintiffs, the Class and Subclasses members' Private Information was without their consent, and in violation of various statutes, regulations and other laws.

653. As a result of the invasion of privacy caused by Blackbaud, Plaintiffs, the Class and Subclass members suffered and will continue to suffer damages and injury as set forth herein.

654. Plaintiffs, the Class and Subclasses members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

655. Plaintiffs and Class members are entitled to injunctive relief requiring Blackbaud to, *e.g.*, (i) identify all legacy data it still maintains; (ii) destroy or encrypt legacy data that has been "at rest" for an unreasonable amount of time; (iii) notify all Social Good Entities and consumers with legacy data that is still be maintained by Blackbaud; (iv) strengthen its data security programs and monitoring procedures; (v) submit to future annual audits of those systems and monitoring procedures; (vi) immediately provide robust and adequate credit monitoring to Plaintiffs and Legacy/Back-up Subclass members; and (iv) correct its past inaccurate and

incomplete statements to Plaintiffs, Class members, government officials, and the general public about the Data Breach, and any other relief this Court deems just and proper.

B. CLAIMS ON BEHALF OF THE STATE SUBCLASSES

**CLAIMS ON BEHALF OF THE ALABAMA SUBCLASS
COUNT 5: ALABAMA DECEPTIVE TRADE PRACTICES ACT,
Ala. Code §§ 8-19-1, ET SEQ.**

656. The Plaintiff(s) identified above (“Plaintiff(s),” for purposes of this Count), individually and on behalf of the Alabama Subclass, repeats and alleges Paragraphs 1-655, as if fully alleged herein. This claim is brought individually under the laws of Alabama and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

657. Blackbaud is a “person” as defined by Ala. Code § 8-19-3(5).

658. Plaintiff(s) and Alabama Subclass members are “consumers” as defined by Ala. Code § 8-19-3(2).

659. Plaintiff(s) sent notice pursuant to Ala. Code § 8-19-10(e) on February 24, 2021.

660. Blackbaud advertised, offered, or sold goods or services in Alabama, and engaged in trade or commerce directly or indirectly affecting the people of Alabama.

661. Blackbaud engaged in deceptive acts and practices in the conduct of trade or commerce, in violation of the Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5, including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and
- c. Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce, including acts and

practices that would violate Section 5(a)(1) of the FTC Act, 15 U.S.C. § 45(a)(1), 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05.

662. Blackbaud's deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Alabama Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alabama Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Alabama Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alabama Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Alabama Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Alabama Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alabama Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05.

663. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

664. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Alabama Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Alabama Subclass members into believing they did not need to take actions to secure their identities.

665. Blackbaud intended to mislead Plaintiff and Alabama Subclass members and induce them to rely on its misrepresentations and omissions.

666. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

667. Instead, Blackbaud continued to be trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs and the Alabama Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public.

668. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Alabama Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

669. Blackbaud acted intentionally, knowingly, and maliciously to violate the Alabama Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs and Alabama Subclass members' rights.

670. As a direct and proximate result of Blackbaud's deceptive acts and practices, Plaintiffs and Alabama Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

671. Blackbaud's deceptive acts and practices caused substantial injury to Plaintiffs, and Alabama Subclass members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

672. Plaintiffs and the Alabama Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of \$100; treble damages; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE ALASKA SUBCLASS

COUNT 6: PERSONAL INFORMATION PROTECTION ACT, Alaska Stat. §§ 45.48.010, ET SEQ.

673. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Alaska Subclass, repeats and alleges Paragraphs 1-672, as if fully alleged herein. This claim is brought individually under the laws of Alaska and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding personal information protection.

674. Blackbaud is a business that owns or licenses Private Information as defined by Alaska Stat. § 45.48.090(7). As such a business, it is a Covered Person as defined in Alaska Stat. § 45.48.010(a).

675. Plaintiff and Alaska Subclass members' Private Information includes Private Information as covered under Alaska Stat. § 45.48.010(a).

676. Blackbaud is required to accurately notify Plaintiff and Alaska Subclass members if it becomes aware of a breach of its data security program in the most expeditious time possible and without unreasonable delay under Alaska Stat. § 45.48.010(b).

677. Blackbaud is similarly required to determine the scope of the breach and restore the reasonable integrity of the information system under Alaska Stat. § 45.48.010(b).

678. Because Blackbaud was aware of a breach of its security system, Blackbaud had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Alaska Stat. § 45.48.010(b).

679. By failing to disclose the Data Breach in a timely and accurate manner Blackbaud violated Alaska Stat. § 45.48.010(b).

680. Pursuant to Alaska Stat. § 45.48.080(b), a violation of Alaska Stat. § 45.48.010(b) is an unfair or deceptive act or practice under the Alaska Unfair Trade Practices and Consumer Protection Act, Alaska Stat. §§ 45.50.471, *et seq.*

681. Additionally, Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Alaska Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Alaska Subclass members into believing they did not need to take actions to secure their identities.

682. As a direct and proximate result of Blackbaud's violations of Alaska Stat. § 45.48.010(b), Plaintiff and Alaska Subclass members suffered damages, as described above.

683. Plaintiff and Alaska Subclass members seek relief measured as the greater of (a) each unlawful act, (b) three times actual damages in an amount to be determined at trial, or (c) statutory damages in the amount of \$500 for Plaintiff and each Alaska Subclass Member; reasonable attorneys' fees; and any other just and proper relief available under Alaska Stat. § 45.48.080(b)(2) and Alaska Stat. § 45.50.531.

COUNT 7: ALASKA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT, Alaska Stat. §§ 45.50.471, ET SEQ.

684. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Alaska Subclass, repeats and alleges Paragraphs 1-683, as if fully alleged herein. This claim is brought individually under the laws of Alaska and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

685. Blackbaud advertised, offered, or sold goods or services in Alaska and engaged in trade or commerce directly or indirectly affecting the people of Alaska.

686. Plaintiffs and Alaska Subclass members are "consumers" as defined by Alaska Stat. § 45.50.561(a)(4).

687. Blackbaud engaged in unfair or deceptive acts and practices in the conduct of trade or commerce, in violation Alaska Stat. § 45.50.471, including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade, when they are of another;
- c. Advertising goods or services with intent not to sell them as advertised;

- d. Engaging in any other conduct creating a likelihood of confusion or of misunderstanding and which misleads, deceives, or damages a buyer in connection with the sale or advertisements of its goods or services; and
- e. Using or employing deception, fraud, false pretense, false promise, misrepresentation, or knowingly concealing, suppressing, or omitting a material fact with intent that others rely upon the concealment, suppression, or omission in connection with the sale or advertisement of its goods or services whether or not a person was in fact misled, deceived, or damaged.

688. Blackbaud's unfair and deceptive acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Alaska Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alaska Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Alaska Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alaska Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Alaska Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Alaska Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alaska Subclass members' Private

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05.

689. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Alaska Subclass members, about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

690. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Alaska Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Alaska Subclass members into believing they did not need to take actions to secure their identities.

691. Blackbaud intended to mislead Plaintiff and Alaska Subclass members and induce them to rely on its misrepresentations and omissions.

692. Blackbaud acted intentionally, knowingly, and maliciously to violate Alaska's Consumer Protection Act, and recklessly disregarded Plaintiff and Alaska Subclass members' rights.

693. As a direct and proximate result of Blackbaud's unfair and deceptive acts and practices, Plaintiff and Alaska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

694. Plaintiff and the Alaska Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) three times their actual damages or (b) statutory

damages in the amount of \$500; punitive damages; reasonable attorneys' fees and costs; injunctive relief; and any other relief that is necessary and proper.

CLAIMS ON BEHALF OF THE ARIZONA SUBCLASS

COUNT 8: ARIZONA CONSUMER FRAUD ACT, Ariz. Rev. Stat. §§ 44-1521, ET SEQ.

695. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Arizona Subclass, repeats and alleges Paragraphs 1-694, as if fully alleged herein. This claim is brought individually under the laws of Arizona and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud.

696. Blackbaud is a "person" as defined by Ariz. Rev. Stat. § 44-1521(6).

697. Blackbaud advertised, offered, or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

698. Blackbaud engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, Ariz. Rev. Stat. § 44-1521(5)) in violation of Ariz. Rev. Stat. § 44-1522(A), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Arizona Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05, which was a direct and proximate cause of the Data Breach;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Arizona Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Arizona Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Arizona Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-05.

699. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

700. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Arizona Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Arizona Subclass members into believing they did not need to take actions to secure their identities.

701. Blackbaud intended to mislead Plaintiff and Arizona Subclass members and induce them to rely on its misrepresentations and omissions.

702. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply

with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Arizona Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Arizona Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

703. Blackbaud acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiff and Arizona Subclass members' rights.

704. As a direct and proximate result of Blackbaud's unfair and deceptive acts and practices, Plaintiff and Arizona Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

705. Plaintiff and Arizona Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE ARKANSAS SUBCLASS

COUNT 9: ARKANSAS DECEPTIVE TRADE PRACTICES ACT, Ark. Code Ann. §§ 4-88-101, ET SEQ.

706. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Arkansas Subclass, repeats and alleges Paragraphs 1-705, as if fully alleged herein. This claim is brought individually under the laws of Arkansas and on behalf

of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

707. Blackbaud is a “person” as defined by Ark. Code Ann. § 4-88-102(5).

708. Blackbaud’s products and services are “goods” and “services” as defined by Ark. Code Ann. §§ 4-88-102(4) and (7).

709. Blackbaud advertised, offered, or sold goods or services in Arkansas and engaged in trade or commerce directly or indirectly affecting the people of Arkansas.

710. The Arkansas Deceptive Trade Practices Act (“ADTPA”), Ark. Code Ann. §§ 4-88-101, *et seq.*, prohibits unfair, deceptive, false, and unconscionable trade practices.

711. Blackbaud engaged in acts of deception and false pretense in connection with the sale and advertisement of services in violation of Ark. Code Ann. § 4-88-1-8(1) and concealment, suppression and omission of material facts, with intent that others rely upon the concealment, suppression or omission in violation of Ark. Code Ann. § 4-88-1-8(2), and engaged in the following deceptive and unconscionable trade practices defined in Ark. Code Ann. § 4-88-107:

- a. Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services and as to goods being of a particular standard, quality, grade, style, or model;
- b. Advertising goods or services with the intent not to sell them as advertised;
- c. Employing consistent bait-and-switch advertising of an attractive but insincere offer to sell a product or service which the seller in truth does not intend or desire to sell, as evidenced by acts demonstrating an intent not to sell the advertised product or services;
- d. Knowingly taking advantage of a consumer who is reasonably unable to protect his or her interest because of ignorance; and
- e. Engaging in other unconscionable, false, or deceptive acts and practices in business, commerce, or trade.
- f. Blackbaud’s unconscionable, false, and deceptive acts and practices include:

- g. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Arkansas Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- h. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- i. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arkansas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-05, and the Arkansas Personal Information Protection Act, Ark. Code Ann. § 4-110-104(b), which was a direct and proximate cause of the Data Breach;
- j. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Arkansas Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- k. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arkansas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Arkansas Personal Information Protection Act, Ark. Code Ann. § 4-110-104(b);
- l. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Arkansas Subclass members of the Data Breach;
- m. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- n. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Arkansas Subclass members' Private Information; and
- o. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arkansas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Arkansas Personal Information Protection Act, Ark. Code Ann. § 4-110-104(b).

712. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

713. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Arkansas Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Arkansas Subclass members into believing they did not need to take actions to secure their identities.

714. Blackbaud intended to mislead Plaintiff and Arkansas Subclass members and induce them to rely on its misrepresentations and omissions.

715. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Arkansas Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Arkansas Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

716. Blackbaud acted intentionally, knowingly, and maliciously to violate Arkansas's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Arkansas Subclass members' rights.

717. As a direct and proximate result of Blackbaud's unconscionable, unfair, and deceptive acts or practices and Plaintiff and Arkansas Subclass members' reliance thereon, Plaintiff and Arkansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including

from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

718. Plaintiff and the Arkansas Subclass members seek all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 10: CALIFORNIA CUSTOMER RECORDS ACT, Cal. Civ. Code §§ 1798.80, *et seq.*

719. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-718, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding customer records.

720. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

721. Blackbaud is a business that owns, maintains, and licenses "personal information", within the meaning of Cal. Civ. Code § 1798.81.5(d)(1), about Plaintiff and California Subclass members.

722. Blackbaud is registered as a “data broker” in California, which is defined as a “business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.” Cal. Civ. Code § 1798.99.80.²⁶³

723. Businesses that own or license computerized data that includes personal information, including SSNs, are required to notify California residents when their personal information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach “in the most expedient time possible and without unreasonable delay.” Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include “the types of Personal Information that were or are reasonably believed to have been the subject of the breach.” Cal. Civ. Code § 1798.82. *Id.*

724. Blackbaud is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82(h).

725. Plaintiff and California Subclass members’ Private Information includes “personal information” as covered by Cal. Civ. Code §§ 1798.81.5(d)(1), 1798.82(h).

726. Because Blackbaud reasonably believed that Plaintiff and California Subclass members’ Private Information was acquired by unauthorized persons during the Data Breach, Blackbaud had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

727. Blackbaud failed to fully disclose material information about the breach.

728. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated Cal. Civ. Code § 1798.82.

²⁶³ *Data Broker Registration for Blackbaud, Inc.*, Cal. Dept. of Justice, <https://oag.ca.gov/data-broker/registration/185724> (last visited Dec. 19, 2021) [<https://perma.cc/HG5C-VRXV>].

729. As a direct and proximate result of Blackbaud’s violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass members suffered damages, as described above.

730. Plaintiff and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

**COUNT 11: CALIFORNIA UNFAIR COMPETITION LAW,
Cal. Bus. & Prof. Code §§ 17200, *et seq.***

731. The California Plaintiffs identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-730, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair competition.

732. Blackbaud is a “person” as defined by Cal. Bus. & Prof. Code §17201.

733. Blackbaud violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* (“UCL”) by engaging in unlawful, unfair, and deceptive business acts and practices.

734. Blackbaud’s “unfair” and “deceptive” acts and practices include:

- a. Blackbaud failed to implement and maintain reasonable security measures to protect Plaintiff and California Subclass members’ Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Blackbaud failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. For example, Blackbaud failed to patch the well-known Apache Struts vulnerability, which made it trivial for a hacker to penetrate Blackbaud’s systems. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass, whose Private Information has been compromised.
- b. Blackbaud’s failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers’ data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including California’s Consumer Legal Remedies Act (“CLRA”), Cal Civ.

Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Confidentiality of Medical Information Act (“CMIA”), Cal Civ. Code § 56.26(b), and California’s Consumer Records Act, Cal. Civ. Code § 1798.81.5.

- c. Blackbaud’s failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Blackbaud’s inadequate security, consumers could not have reasonably avoided the harms that Blackbaud caused.
- d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

735. Blackbaud has engaged in “unlawful” business practices by violating multiple laws, including the CCRA, Cal. Civ. Code §§ 1798.80, *et seq.*, the CLRA, Cal. Civ. Code §§ 1780, *et seq.*, 15 U.S.C. § 680, *et seq.*, the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

736. Blackbaud’s unlawful practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members’ Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d., COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b), which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and California Subclass members’ Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass

- members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b);
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and California Subclass members of the Data Breach;
 - g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
 - h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and California Subclass members' Private Information; and
 - i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

737. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

738. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the California Subclass members, into believing that their Private Information was not exposed and misled Plaintiffs and the California Subclass members into believing they did not need to take actions to secure their identities.

739. As a direct and proximate result of Blackbaud's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California Subclass members were injured and lost money or property, including monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Private Information, including but not limited to the

diminishment of their present and future property interest in their Private Information and the deprivation of the exclusive use of their Private Information.

740. Blackbaud acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs and California Subclass members' rights.

741. Plaintiffs and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Blackbaud's unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

**COUNT 12: CALIFORNIA CONSUMER LEGAL REMEDIES ACT,
Cal. Civ. Code §§ 1750, *et seq.***

742. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-741, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer legal remedies.

743. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

744. Blackbaud is a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770. Specifically, Blackbaud

provides cloud-based computing services to customers that involve storing and managing Private Information for use by consumers and direct customers such as Social Good Entities.

745. As part of the services Blackbaud offers, Blackbaud touts its ongoing efforts to keep consumers' Private Information secure, including by ensuring ongoing compliance with legal privacy standards established both domestically and abroad, as recognized by Blackbaud's Privacy Shield Notice. Indeed, Blackbaud purports to "tirelessly track and interpret pending legislation to ensure that that Blackbaud provides the features [customers] need to protect the privacy of [their] constituents while managing data in a compliant way. As privacy legislation evolves, [Blackbaud's] products do too."

746. Plaintiffs and the California Class are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

747. Blackbaud's acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade when they were not;
- c. Advertising goods or services with intent not to sell them as advertised; and
- d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.
- e. Blackbaud violated Civil Code § 1770, in the following ways:
- f. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- g. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security

- and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- h. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d., COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b), which was a direct and proximate cause of the Data Breach;
 - i. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and California Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
 - j. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b);
 - k. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and California Subclass members of the Data Breach;
 - l. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
 - m. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and California Subclass members' Private Information; and
 - n. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

748. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

749. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the California Subclass members, into believing that their Private Information was not exposed and misled Plaintiffs and the California Subclass members into believing they did not need to take actions to secure their identities.

750. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the California Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the California Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

751. As a direct and proximate result of Blackbaud's violations of California Civil Code § 1770, Plaintiffs and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information, including but not limited to the diminishment of their present and future property interest in their Private Information and the deprivation of the exclusive use of their Private Information.

752. Plaintiffs and the California Subclass have provided notice of their claims for damages to Blackbaud, in compliance with California Civil Code § 1782(a), on February 24, 2021. Blackbaud responded on March 8, 2021; however, such response did not offer or provide an adequate remedy at law.

753. Plaintiffs and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

**COUNT 13: CALIFORNIA CONSUMER PRIVACY ACT,
Cal. Civ. Code §§ 1798.100, *et seq.***

754. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-753, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer privacy.

755. Plaintiffs and California Subclass members are residents of California.

756. Blackbaud is a corporation that is organized or operated for the profit or financial benefit of its shareholders or other owners, with annual gross revenues over \$25 million.

757. Blackbaud is a business that collects consumers' personal information as defined by Cal. Civ. Code § 1798.140(e). Specifically, Blackbaud obtains, receives, or accesses consumers' personal information when customers use Blackbaud's products to maintain and process consumer data.

758. Blackbaud and its direct customers determine the purposes and means of processing consumers' personal information. Blackbaud uses consumers' personal data to provide services at customers' requests, as well as to develop, improve, and test Blackbaud's services.

759. Blackbaud is registered as a "data broker" in California, which is defined as a "business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code § 1798.99.80.

760. Blackbaud violated Section 1798.150 of the California Consumer Privacy Act by failing to prevent Plaintiffs and the California Subclass members' nonencrypted and nonredacted personal information from unauthorized access and exfiltration, theft, or disclosure as a result of Blackbaud's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

761. Blackbaud knew or should have known that its data security practices were inadequate to secure California Subclass members' Private Information and that its inadequate data security practices gave rise to the risk of a data breach.

762. Blackbaud failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the Private Information it collected and stored.

763. The cybercriminals accessed "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d), in the Data Breach.

764. Upon information and belief, Plaintiff and California Subclass members' Private Information accessed by the cybercriminals in the Data Breach includes "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d).

765. Plaintiffs seek injunctive relief in the form of an order requiring Blackbaud to employ adequate security practices consistent with law and industry standards to protect the California Subclass members' Private Information, requiring Blackbaud to complete its investigation, and to issue an amended statement giving a detailed explanation that confirms, with reasonable certainty, what categories of data were stolen and accessed without the California Subclass members' authorization, along with an explanation of how the data breach occurred.

766. Plaintiffs and the California Subclass members seek statutory damages or actual damages, whichever is greater, pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

767. As a direct and proximate result of Blackbaud's violations of the Cal. Civ. Code §§ 1798.150, Plaintiff and California Subclass members suffered damages, as described above.

768. On September 9, 2020, counsel for Mamie Estes served written notice identifying Blackbaud's violations of Cal. Civil Code § 1798.150(a) and demanding the data breach be cured, pursuant to Cal. Civil Code § 1798.150(b). On September 11, 2020, counsel for Philip Eisen, Mamie Estes, and Kassandra Clayton, respectively, did the same. Because Blackbaud has neither cured the noticed violation nor provided the Plaintiffs with an express written statement that the violations have been cured and that no further violations shall occur, Plaintiff and the California Subclass seek statutory damages pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

769. Additionally, Blackbaud has failed to cure the violation of the CCPA.

**COUNT 14: CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT,
Cal. Civil Code § 56, *et seq.***

770. Plaintiff Clayton, individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-769, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer privacy.

771. The California's Confidentiality of Medical Information Act ("CMIA") prohibits, among other things, unauthorized disclosure of private medical information. Cal. Civ. Code §§ 56, *et seq.*

772. Plaintiff Clayton provided PHI to a Social Good Entity which is a "health care practitioner" is a "provider of health care" as defined by Cal. Civ. Code § 56.05(j).

773. Plaintiff Clayton is a "patient" as defined by Cal. Civ. Code § 56.05(k).

774. Blackbaud is a “provider of health care” subject to the CMIA because it is a “business that offers software or hardware to consumers, . . . that is designed to maintain medical information” in order to make the information available to an individual or Social Good Entity to which Plaintiff provided her PHI. Cal. Civ. Code § 56.06(b).

775. Blackbaud stored in electronic form on its computer system Plaintiff’s “medical information” as defined by Cal. Civ. Code § 56.05(j).

776. Blackbaud’s systems were designed, in part, to make medical information available to Social Good Entities by providing cloud-based computing solutions through which those organizations could store, access, and manage consumers’ medical information, including but not limited to diagnosing, treating, or managing consumers’ medical conditions.

777. Plaintiff did not provide Blackbaud authorization nor was Blackbaud otherwise authorized to disclose Plaintiff’s medical information to an unauthorized third-party.

778. As described throughout this Complaint, Blackbaud negligently maintained, disclosed and released Plaintiff and the California PHI Subclass members’ medical information inasmuch as it did not implement adequate security protocols to prevent unauthorized access to medical information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data the risks of any data breach or otherwise comply with HIPAA data security requirements.

779. As a direct and proximate result of Blackbaud’s negligence, it disclosed and released Plaintiff and the California PHI Subclass members’ medical information to an unauthorized third-party.

780. Blackbaud’s unauthorized disclosure of medical records has caused injury to the Plaintiff and the California PHI Subclass.

781. Upon information and belief, Plaintiff's confidential medical information was viewed by an unauthorized third party.

782. Accordingly, Plaintiff Clayton, individually and on behalf of members of the California PHI Subclass, seek to recover actual, nominal (including \$1000 nominal damages per disclosure under § 56.36(b)), and statutory damages (including under § 56.36(c)) where applicable, together with reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE COLORADO SUBCLASS

COUNT 15: COLORADO SECURITY BREACH NOTIFICATION ACT, Colo. Rev. Stat. §§ 6-1-716, *et seq.*

783. The Colorado Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and alleges Paragraphs 1-782, as if fully alleged herein. This claim is brought individually under the laws of Colorado and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding security breach notification.

784. Blackbaud is a business that owns or licenses computerized data that includes Personal Information as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

785. Plaintiff and Colorado Subclass members' Private Information includes "Personal Information" as covered by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

786. Blackbaud is required to accurately notify Plaintiff and Colorado Subclass members if it becomes aware of a breach of its data security program in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

787. Because Blackbaud was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

788. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated Colo. Rev. Stat. § 6-1-716(2).

789. As a direct and proximate result of Blackbaud's violations of Colo. Rev. Stat. § 6-1-716(2), Plaintiff and Colorado Subclass members suffered and will continue to suffer damages, as described above.

790. Plaintiff and Colorado Subclass members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

**COUNT 16: COLORADO CONSUMER PROTECTION ACT,
Colo. Rev. Stat. §§ 6-1-101, *et seq.***

791. The Colorado Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and alleges Paragraphs 1-790, as if fully alleged herein. This claim is brought individually under the laws of Colorado and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

792. Blackbaud is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

793. Blackbaud engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

794. Plaintiff and Colorado Subclass members, as well as the general public, are actual or potential consumers of the products and services offered by Blackbaud or successors in interest to actual consumers.

795. Blackbaud engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

- a. Knowingly making a false representation as to the characteristics of products and services;
- b. Representing that services are of a particular standard, quality, or grade, though Blackbaud knew or should have known that there were or another;

- c. Advertising services with intent not to sell them as advertised; and
- d. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.
- e. Blackbaud's deceptive trade practices include:
- f. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Colorado Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- g. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- h. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- i. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Colorado Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- j. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- k. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Colorado Subclass members of the Data Breach;
- l. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- m. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Colorado Subclass members' Private Information; and
- n. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

796. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

797. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Colorado Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Colorado Subclass members into believing they did not need to take actions to secure their identities.

798. Blackbaud intended to mislead Plaintiff and Colorado Subclass members and induce them to rely on its misrepresentations and omissions.

799. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Colorado Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Colorado Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

800. Blackbaud acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff and Subclass members' rights.

801. As a direct and proximate result of Blackbaud's deceptive trade practices, Colorado Subclass members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their personal information.

802. Blackbaud's deceptive trade practices significantly impact the public, because nearly all members of the public are actual or potential consumers of Blackbaud's services and the Data Breach affected more than 147 million Americans, including 2.5 million Coloradans.

803. Plaintiff and Colorado Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) \$500, or (c) three times actual damages (for Blackbaud's bad faith conduct); injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE CONNECTICUT SUBCLASS

COUNT 17: BREACH OF SECURITY REGARDING COMPUTERIZED DATA, C.G.S.A. § 36a-701b

804. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Connecticut Subclass, repeats and alleges Paragraphs 1-803, as if fully alleged herein. This claim is brought individually under the laws of Connecticut and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding computerized data.

805. Blackbaud is a business that conducts business in Connecticut and owns, licenses, and maintains computerized data that includes personal information as covered by C.G.S.A. § 36a-701b(b). Blackbaud also maintains computerized data that includes personal information that it does not own as covered by C.G.S.A. § 36a-701b(c).

806. Plaintiff and Connecticut Subclass members' Private Information includes "personal information" as covered by C.G.S.A. § 36a-701b(a).

807. Blackbaud is required to accurately notify Plaintiff and Connecticut Subclass members if it becomes aware of a breach of its data security program in the most expedient time possible and without unreasonable delay, not to exceed ninety days after discovery of the breach under C.G.S.A. § 36a-701b(b).

808. Blackbaud is required to immediately notify Plaintiff and Connecticut Subclass members if it becomes aware of a breach of its data security program which may have compromised personal information Blackbaud stores but Plaintiff and Connecticut Class members own under C.G.S.A. § 36a-701b(c).

809. Because Blackbaud was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by C.G.S.A. §§ 36a-701b(b) and (c).

810. By failing to disclose the Data Breach in an accurate and timely manner, Blackbaud failed to comply with C.G.S.A. §§ 36a-701b(b) and (c). Pursuant to C.G.S.A. § 36a-701b(g), Blackbaud's failure to comply was an unfair trade practice under the Connecticut Unfair Trade Practices Act, C.G.S.A. §§ 42-110a, *et seq.*

811. As a direct and proximate result of Blackbaud's violations of C.G.S.A. §§ 36a-701b(b) and (c), Plaintiff and Connecticut Subclass members suffered damages, as described above.

812. Plaintiff and Connecticut Subclass members seek relief under C.G.S.A. § 42-110g for the harm they suffered because of Blackbaud's violations of C.G.S.A. §§ 36a-701b(b) and (c), including actual damages and equitable relief.

813. Plaintiff repeats and realleges the allegations set forth above as though fully set forth herein.

814. CUTPA's purpose, consistent with its remedial character, is to protect the public from unfair practices in the conduct of any trade or commerce. The statute provides that "[n]o person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Conn. Gen. Stat. § 42-110b

815. Blackbaud has acted, as alleged herein, in the conduct of trade or commerce as defined in Conn. Gen. Stat. § 42-110a(4).

816. Blackbaud's actions, as described herein, have offended public policy.

817. Blackbaud's practices, as outlined above, also violate the Connecticut Computerized Data Act, Conn. Gen. Stat. § 36a-701b et seq.

818. Blackbaud's conduct is part of a general business practice that constitutes unfair and deceptive acts in violation of Conn. Gen. Stat. § 42-110b(a).

819. As a direct and proximate result of Blackbaud's violation of the Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110b(a), Plaintiff and the Class members have suffered ascertainable losses under Conn. Gen. Stat. § 42-110g(a) in an amount to be proven at trial, and they will continue to suffer losses in the future.

820. As a result of Blackbaud's unfair and/or deceptive acts or practices, Blackbaud has reaped ill-gotten profits and gains, which they otherwise would not have received and which, in equity, they should be required to disgorge.

821. Blackbaud is also liable for injunctive and other equitable relief.

822. Blackbaud is also liable, pursuant to Conn. Gen. Stat. § 42-110g(a), for punitive damages.

823. Furthermore, Blackbaud is liable, pursuant to Conn. Gen. Stat. § 42-110g(d), for costs and reasonable attorneys' fees.

824. In compliance with Connecticut General Statutes § 42-110g(c), a copy of this Complaint has been mailed to the Attorney General of the State of Connecticut and the Commissioner of Consumer Protection on this date.

CLAIMS ON BEHALF OF THE DELAWARE SUBCLASS

COUNT 18: DELAWARE COMPUTER SECURITY BREACH ACT, 6 Del. Code Ann. §§ 12b-102, *et seq.*

825. The Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Delaware Subclass, repeats and alleges Paragraphs 1-824, as if fully alleged herein. This claim is brought individually under the laws of Delaware and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding computer security.

826. Blackbaud is a business that owns or licenses computerized data that includes “personal information” as defined by 6 Del. Code Ann. § 12B-102(a).

827. Plaintiff and Delaware Subclass members’ Private Information includes “personal information” covered under 6 Del. Code Ann. § 12B-101(4).

828. Blackbaud is required to accurately notify Plaintiff and Delaware Subclass members if Blackbaud becomes aware of a breach of its data security program which is reasonably likely to result in the misuse of a Delaware resident’s Private Information, in the most expedient time possible and without unreasonable delay under 6 Del. Code Ann. § 12B-102(a).

829. Because Blackbaud was aware of a breach of its security system which is reasonably likely to result in misuse of Delaware residents’ Private Information, Blackbaud had an obligation to disclose the data breach in a timely and accurate fashion as mandated by 6 Del. Code Ann. § 12B-102(a).

830. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated 6 Del. Code Ann. § 12B-102(a).

831. As a direct and proximate result of Blackbaud's violations of 6 Del. Code Ann. §12B-102(a), Plaintiff and Delaware Subclass members suffered damages and will continue to suffer damages, as described above.

832. Plaintiff and Delaware Subclass members seek relief under 6 Del. Code Ann. § 12B-104, including actual damages and equitable relief.

**COUNT 19: DELAWARE CONSUMER FRAUD ACT,
6 Del. Code §§ 2513, *et seq.***

833. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Delaware Subclass, repeats and alleges Paragraphs 1-832, as if fully alleged herein. This claim is brought individually under the laws of Delaware and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud.

834. Blackbaud is a "person" that is involved in the "sale" of "merchandise," as defined by 6 Del. Code § 2511(7), (8), and (6).

835. Blackbaud advertised, offered, or sold goods or services in Delaware and engaged in trade or commerce directly or indirectly affecting the people of Delaware.

836. Blackbaud used and employed deception, fraud, false pretense, false promise, misrepresentation, and the concealment, suppression, and omission of material facts with intent that others rely upon such concealment, suppression and omission, in connection with the sale and advertisement of merchandise, in violation of 6 Del. Code § 2513(a), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Delaware Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Delaware's data security statute, 6 Del. Code § 12B-100, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Delaware Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Delaware's data security statute, 6 Del. Code § 12B-100;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Delaware Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Delaware Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Delaware's data security statute, 6 Del. Code § 12B-100.

837. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

838. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Delaware Subclass members, that

their Private Information was not exposed and misled Plaintiffs and the Delaware Subclass members into believing they did not need to take actions to secure their identities.

839. Blackbaud acted intentionally, knowingly, and maliciously to violate Delaware's Consumer Fraud Act, and recklessly disregarded Plaintiff and Delaware Subclass members' rights.

840. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Delaware Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Delaware Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

841. Blackbaud's unlawful trade practices were gross, oppressive, and aggravated, and Blackbaud breached the trust of Plaintiff and the Delaware Subclass members.

842. As a direct and proximate result of Blackbaud's unlawful acts and practices, Plaintiff and Delaware Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

843. Plaintiff and Delaware Subclass members seek all monetary and non-monetary relief allowed by law, including damages under 6 Del. Code § 2525 for injury resulting from the direct and natural consequences of Blackbaud's unlawful conduct; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE DISTRICT OF COLUMBIA SUBCLASS

COUNT 20: DISTRICT OF COLUMBIA CONSUMER SECURITY BREACH NOTIFICATION ACT, D.C. Code §§ 28-3851, *et seq.*

844. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the District of Columbia Subclass, repeats and alleges Paragraphs 1-843, as if fully alleged herein. This claim is brought individually under the laws of the District of Columbia and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding data security breach notification.

845. Blackbaud is a business that owns or licenses computerized data that includes Private Information as defined by D.C. Code § 28-3852(a).

846. Plaintiff and District of Columbia Subclass members' Private Information includes Private Information as covered under D.C. Code § 28-3851(3).

847. Blackbaud is required to accurately notify Plaintiff and District of Columbia Subclass members if it becomes aware of a breach of its data security program in the most expedient time possible and without unreasonable delay under D.C. Code § 28-3852(a).

848. Because Blackbaud was aware of a breach of its security system, Blackbaud had an obligation to disclose the data breach in a timely and accurate fashion as mandated by D.C. Code § 28-3852(a).

849. By failing to disclose the Data Breach in a timely and accurate manner Blackbaud violated D.C. Code § 28-3852(a).

850. As a direct and proximate result of Blackbaud's violations of D.C. Code § 28-3852(a), Plaintiff and District of Columbia Subclass members suffered damages and will continue to suffer damages, as described above.

851. Plaintiff and District of Columbia Subclass members seek relief under D.C. Code § 28-3853(a), including actual damages.

COUNT 21: DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT, D.C. code §§ 28-3904, *et seq.*

852. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the District of Columbia Subclass, repeats and alleges Paragraphs 1-851, as if fully alleged herein. This claim is brought individually under the laws of District of Columbia and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

853. Blackbaud is a "person" as defined by D.C. Code § 28-3901(a)(1).

854. Blackbaud is a "merchant" as defined by D.C. Code § 28-3901(a)(3).

855. Plaintiff and District of Columbia Subclass members are "consumers" who purchased or received goods or services for personal, household, or family purposes, as defined by D.C. Code § 28-3901.

856. Blackbaud advertised, offered, or sold goods or services in District of Columbia and engaged in trade or commerce directly or indirectly affecting the people of District of Columbia.

857. Blackbaud engaged in unfair, unlawful, and deceptive trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of D.C. Code § 28-3904, including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, grade, style, or model, when they are of another;
- c. Misrepresenting a material fact that has a tendency to mislead;
- d. Failing to state a material fact where the failure is misleading;
- e. Advertising or offering goods or services without the intent to sell them as advertised or offered; and
- f. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

858. Blackbaud's unfair, unlawful, and deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and District of Columbia Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and District of Columbia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and District of Columbia Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and District of Columbia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and District of Columbia Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and District of Columbia Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and District of Columbia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

859. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

860. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the District of Columbia Subclass members, that their Private Information was not exposed and misled Plaintiffs and the District of Columbia Subclass members into believing they did not need to take actions to secure their identities.

861. Blackbaud intended to mislead Plaintiff and District of Columbia Subclass members and induce them to rely on its misrepresentations and omissions.

862. The above unfair and deceptive practices and acts by Blackbaud were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and District of Columbia Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

863. Blackbaud acted intentionally, knowingly, and maliciously to violate the District of Columbia's Consumer Protection Procedures Act, and recklessly disregarded Plaintiff and District of Columbia Subclass members' rights.

864. As a direct and proximate result of Blackbaud's unfair, unlawful, and deceptive trade practices, Plaintiff and District of Columbia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

865. Plaintiff and District of Columbia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, injunctive relief, punitive damages, attorneys' fees and costs, the greater of treble damages or \$1500 per violation, and any other relief that the Court deems proper.

CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS

COUNT 22: FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, Fla. Stat. §§ 501.201, *et seq.*

866. The Florida Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Florida Subclass, repeats and alleges Paragraphs 1-865, as if fully alleged herein. This claim is brought individually under the laws of Florida and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive and unfair trade practices.

867. This cause of action is brought pursuant to the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. § 501.201 *et seq.* The stated purpose of this Act is to "protect the consuming public . . . from those who engage in unfair methods of competition, or

unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce.”

Id. § 501.202(2).

868. Plaintiff and Florida Subclass members are “consumers” as defined by Fla. Stat. § 501.203.

869. Blackbaud advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

870. Blackbaud engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Florida Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Florida’s data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Florida Subclass members’ Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Florida’s data security statute, F.S.A. § 501.171(2);
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Florida Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Florida Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Florida's data security statute, F.S.A. § 501.171(2).

871. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

872. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Florida Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Florida Subclass members into believing they did not need to take actions to secure their identities.

873. Blackbaud had exclusive knowledge of material facts concerning the inadequate security and vulnerabilities of its systems and networks that contained Plaintiff and Florida Subclass members' Private Information, including that such information was vulnerable to cyberattack, unauthorized access, exfiltration, and misuse.

874. Prior to the Data Breach, Blackbaud had been repeatedly notified from employees that its systems and networks were vulnerable to cyberattack and that such cyberattack would likely be successful.

875. Despite Blackbaud's exclusive knowledge of material facts that its systems and networks that contained Plaintiff and Florida Subclass members' Private Information were not adequately secure and were vulnerable to cyberattack, Blackbaud actively concealed such information from Plaintiff, Florida Subclass members and Social Good Entities.

876. Blackbaud had exclusive knowledge of material facts concerning when and what Private Information was accessed and exfiltrated during the Data Breach; however, Blackbaud actively concealed such information from Plaintiff, Florida Subclass members, and Social Good Entities, and otherwise misrepresented that certain Private Information was not accessed and exfiltrated.

877. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

878. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Florida Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public.

879. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Florida Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

880. As a direct and proximate result of Blackbaud's unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

881. Plaintiff and Florida Subclass members seek declaratory and injunctive relief as well as reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE GEORGIA SUBCLASS

COUNT 23: GEORGIA SECURITY BREACH NOTIFICATION ACT, O.C.G.A. §§ 10-1-912, *et seq.*

882. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and alleges Paragraphs 1-881, as if fully alleged herein. This claim is brought individually under the laws of Georgia and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding security breach notification.

883. Blackbaud is a business that owns or licenses computerized data that includes "personal information" as defined by O.C.G.A. § 10-1-912(a).

884. Plaintiff and Georgia Subclass members' Private Information includes "personal information" as covered under O.C.G.A. § 10-1-912(a).

885. Blackbaud is required to accurately notify Plaintiff and Georgia Subclass members if it becomes aware of a breach of its data security program that was reasonably likely to have caused unauthorized persons to acquire Plaintiff and Georgia Subclass members' Private Information, in the most expedient time possible and without unreasonable delay under O.C.G.A. § 10-1-912(a).

886. Because Blackbaud was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff and Georgia Subclass members' Private Information, Blackbaud had an obligation to disclose the data breach in a timely and accurate fashion as mandated by O.C.G.A. § 10-1-912(a).

887. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated O.C.G.A. § 10-1-912(a).

888. As a direct and proximate result of Blackbaud's violations of O.C.G.A. § 10-1-912(a), Plaintiff and Georgia Subclass members suffered damages, and will continue to suffer damages, as described above.

889. Plaintiff and Georgia Subclass members seek relief under O.C.G.A. § 10-1-912 including actual damages and injunctive relief.

**COUNT 24: GEORGIA FAIR BUSINESS PRACTICES ACT,
O.C.G.A. § 10-1-390, *et seq.***

890. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and alleges Paragraphs 1-889, as if fully alleged herein. This claim is brought individually under the laws of Georgia and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding fair business practices.

891. Blackbaud's conduct described herein constitutes deceptive acts and practices, which were directed at Plaintiffs and Georgia Subclass members, and are violations of Georgia Fair Business Practices Act, O.C.G.A. § 10-1-390, *et seq.* ("FBPA").

892. Blackbaud, Plaintiffs, and Class members are "persons" within the meaning of the Georgia Fair Business Practices Act ("GFBPA"), O.C.G.A. § 10-1-399(a).

893. Blackbaud is engaged in, and its acts and omissions affect, trade and commerce under O.C.G.A. § 10-1-392(28). Further, Blackbaud is engaged in "consumer acts or practices," which are defined as "acts or practices intended to encourage consumer transactions" under O.C.G.A. § 10-1-392(7). Blackbaud, in its capacity as a "consumer reporting agency," generates

and maintains “consumer reports” and “files” subject to the GFBPA. O.C.G.A. §10-1-392 (9)-(10), (14).

894. Blackbaud’s acts, practices, and omissions at issue in this matter were directed to Plaintiffs and Georgia Subclass members.

895. At the time of its misrepresentations and omissions, Blackbaud was either aware that it was failing to adequately maintain and secure Private Information, that the Private Information exposed during the Data Breach did include sensitive Private Information, or was aware that it lacked the information and/or knowledge required to make such a representation truthfully. Blackbaud concealed, omitted and failed to disclose this information to Plaintiffs and Class Members.

896. Blackbaud engaged in “[u]nfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce” in violation of O.C.G.A. § 10-1-393(a). Those acts and practices include those expressly declared unlawful by O.C.G.A. § 10-1-393(b), such as:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade if they are of another; and
- c. Advertising goods or services with intent not to sell them as advertised.

897. In addition, Blackbaud engaged in the unfair and deceptive acts and practices described below that, while not expressly declared unlawful by O.C.G.A. § 10-1-393(b), are prohibited by O.C.G.A. § 10-1-393(a).

898. In the course of its business, Blackbaud engaged in unfair acts and practices prohibited by O.C.G.A. § 10-1-393(a), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members’ Private Information,

- which was a direct and proximate cause of the Data Breach and its immense scope;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, adequately improve security and privacy measures following previous cybersecurity incidents, and detect and redress the Data Breach while it was ongoing, which were a direct and proximate cause of the Data Breach and its immense scope; and
 - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach and its immense scope.

899. In the course of its business, Blackbaud also engaged in deceptive acts and practices prohibited by O.C.G.A. § 10-1-393(a), including:

- a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class members' Private Information, including by implementing and maintaining reasonable security measures;
- b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- c. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Georgia Subclass members of the Data Breach;
- d. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' Private Information; and
- f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security of Plaintiffs and Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

900. The misrepresentations and omissions described in the preceding paragraph were material and made intentionally and knowingly with the intent that Plaintiffs, Class members, and others (such as its customers, regulators, investors, and those who otherwise used data from

Blackbaud for business purposes) rely upon them in connection with accessing and storing the extremely sensitive and valuable Private Information of Plaintiffs and Class members.

901. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Georgia Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Georgia Subclass members into believing they did not need to take actions to secure their identities.

902. Prior to the Data Breach, Blackbaud knew of the inadequate security controls and vulnerabilities in its systems and networks containing Plaintiff and the Georgia Subclass members' sensitive and valuable Private Information, but failed to remedy the inadequacies to protect this information.

903. Blackbaud's deceptive acts and practices were likely to and did in fact deceive the public at large and reasonable consumers, including Plaintiffs and Georgia Subclass members, regarding the security and safety of the Private Information in its care, including the Private Information of Plaintiffs and Georgia Subclass members. Blackbaud's deceptive acts and practices also were intended to and did in fact deceive others who relied upon Blackbaud to maintain the security of the Private Information in its care, including its customers, regulators, and others who used data from Blackbaud for business purposes.

904. Blackbaud's representations and omissions were material to Plaintiffs, the Georgia Subclass and others (such as the Social Good Entities, regulators, and others who used data from Blackbaud for business purposes) given the extreme sensitivity, value, and importance of the Private Information maintained by Blackbaud; the uncertainty and disruption that would inevitably occur if the marketplace were informed Blackbaud did not adequately protect Private Information;

and the obvious adverse consequences to participants in the American economy from a substantial data breach at Blackbaud.

905. Blackbaud knew or should have known that by collecting, selling, and trafficking in Private Information, Plaintiffs, Georgia Subclass members, and others (such as the Social Good Entities, regulators, and others who used data from Blackbaud for business purposes) would reasonably rely upon and assume Blackbaud's data systems were secure unless Blackbaud otherwise informed them.

906. Because Blackbaud's primary product was the sale and analysis of highly sensitive Private Information, and because Blackbaud controlled the compilation of and access to such Private Information, Plaintiffs, Georgia Subclass members, and others involved (such as Blackbaud's customers, regulators, and others who used data from Blackbaud for business purposes) relied upon Blackbaud to advise if its data systems were not secure and, thus, Private Information could be compromised.

907. Plaintiffs, Georgia Subclass members, and others who relied upon Blackbaud to maintain adequate data security programs had no effective means on their own to discover the truth. In particular, Blackbaud did not afford Plaintiffs and Georgia Subclass members any opportunity to inspect Blackbaud's data security, learn that it was inadequate and non-compliant with legal requirements, or otherwise ascertain the truthfulness of Blackbaud's representations and omissions regarding Blackbaud's ability to protect data and comply with the law.

908. Plaintiffs, Georgia Subclass members, and others (such as the Social Good Entities, regulators, and others who used data from Blackbaud for business purposes) relied to their detriment upon Blackbaud's representations and omissions regarding data security, including

Blackbaud's failure to alert customers that its privacy and security protections were inadequate and insecure and thus were vulnerable to attack.

909. Had Blackbaud disclosed to Plaintiffs, Georgia Subclass members, and others (such as the Social Good Entities, regulators, and others who used data from Blackbaud for business purposes) that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

910. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs and the Georgia Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public.

911. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs and the Georgia Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

912. Blackbaud acted intentionally, knowingly, and maliciously to violate the GFBPA, and recklessly disregarded Plaintiffs and Class members' rights.

913. Blackbaud's violations present a continuing risk to Plaintiffs and Georgia Subclass members, as well as to the general public.

914. Blackbaud's unlawful acts and practices complained of herein affect the consumer marketplace and the public interest, including the millions of U.S. residents, which include Georgians affected by the Data Breach.

915. But for Blackbaud's violations of the GFBPA described above, the Data Breach would not have occurred.

916. As a direct and proximate result of Blackbaud's violations of the GFBPA, Plaintiffs and Georgia Subclass members have suffered injury-in-fact, monetary, and non-monetary damages, including damages from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information, and/or actual damages, as described herein.

917. The GFBPA permits any person who suffers injury or damages as a result of the violation of its provisions to bring an action against the person or persons engaged in such violations. O.C.G.A. § 10-1-399(a).

918. Pursuant to O.C.G.A. § 10-1-399(b), on February 24, 2021, at least 30 days prior to bringing this claim, Plaintiffs and the Georgia Subclass provided Blackbaud with a written demand for relief describing the unfair or deceptive act or practice relied upon and the injury suffered by them. More than 30 days have elapsed since the service of that written demand. No written tender of settlement has been made by Blackbaud.

919. Plaintiffs bring this action on behalf of themselves and Georgia Subclass members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers and the public at large to make informed decisions related to the security of their sensitive Private Information, and to protect the public from Blackbaud's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices.

920. Plaintiffs and Georgia Subclass members are entitled to a judgment against Blackbaud for actual and consequential damages; general, nominal, exemplary, and trebled

damages and attorneys' fees pursuant to the GFBPA; costs; and such other further relief as the Court deems just and proper.

**COUNT 25: GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT,
O.C.G.A. §§ 10-1-370, *et seq.***

921. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and alleges Paragraphs 1-920, as if fully alleged herein. This claim is brought individually under the laws of Georgia and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

922. Blackbaud, Plaintiff, and Georgia Subclass members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

923. Blackbaud engaged in deceptive trade practices in the conduct of its business, in violation of O.C.G.A. § 10-1-372(a), including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised; and
- d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

924. Blackbaud's deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Georgia Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Georgia Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Georgia Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Georgia Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

925. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

926. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Georgia Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Georgia Subclass members into believing they did not need to take actions to secure their identities.

927. Blackbaud intended to mislead Plaintiff and Georgia Subclass members and induce them to rely on its misrepresentations and omissions.

928. In the course of its business, Blackbaud engaged in activities with a tendency or capacity to deceive.

929. Blackbaud acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Georgia Subclass members' rights.

930. Had Blackbaud disclosed to Plaintiffs and Georgia Subclass members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs the Georgia Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Georgia Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

931. As a direct and proximate result of Blackbaud's deceptive trade practices, Plaintiff and Georgia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

932. Plaintiff and Georgia Subclass members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under O.C.G.A. § 10-1-373.

CLAIMS ON BEHALF OF THE HAWAII SUBCLASS

COUNT 26: HAWAII SECURITY BREACH NOTIFICATION ACT, Haw. Rev. Stat. §§ 487N-1, *et seq.*

933. The Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges Paragraphs 1-932, as if fully alleged herein. This claim is brought individually under the laws of Hawaii and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding security breach notification.

934. Blackbaud is a business that owns or licenses computerized data that includes “personal information” as defined by Haw. Rev. Stat. § 487N-2(a).

935. Plaintiff and Hawaii Subclass members’ Private Information includes “personal information” as covered under Haw. Rev. Stat. § 487N-2(a).

936. Blackbaud is a business that owns or licenses computerized data that includes “personal information” as defined by Haw. Rev. Stat. § 487N-2(a).

937. Plaintiff and Hawaii Subclass members’ Private Information includes “personal information” as covered under Haw. Rev. Stat. § 487N-2(a).

938. Blackbaud is required to accurately notify Plaintiff and Hawaii Subclass members if it becomes aware of a breach of its data security program without unreasonable delay under Haw. Rev. Stat. § 487N-2(a).

939. Because Blackbaud was aware of a breach of its security system, it had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Haw. Rev. Stat. § 487N-2(a).

940. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated Haw. Rev. Stat. § 487N-2(a).

941. As a direct and proximate result of Blackbaud's violations of Haw. Rev. Stat. § 487N-2(a), Plaintiff and Hawaii Subclass members suffered damages and will continue to suffer damages, as described above.

942. Plaintiff and Hawaii Subclass members seek relief under Haw. Rev. Stat. § 487N-3(b), including actual damages.

**COUNT 27: HAWAII UNFAIR PRACTICES AND UNFAIR COMPETITION ACT,
Haw. Rev. Stat. §§ 480-1, *et seq.***

943. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges Paragraphs 1-942, as if fully alleged herein. This claim is brought individually under the laws of Hawaii and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair practices and unfair competition.

944. Plaintiff and Hawaii Subclass members are "consumers" as defined by Haw. Rev. Stat. § 480-1.

945. Plaintiffs, the Hawaii Subclass members, and Blackbaud are "persons" as defined by Haw. Rev. Stat. § 480-1.

946. Blackbaud advertised, offered, or sold goods or services in Hawaii and engaged in trade or commerce directly or indirectly affecting the people of Hawaii.

947. Blackbaud engaged in unfair or deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services purchased by Hawaii Subclass members in violation of Haw. Rev. Stat. § 480-2(a), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Hawaii Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Hawaii Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Hawaii Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Hawaii Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

948. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

949. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Hawaii Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Hawaii Subclass members into believing they did not need to take actions to secure their identities.

950. Blackbaud intended to mislead Plaintiff and Hawaii Subclass members and induce them to rely on its misrepresentations and omissions.

951. The foregoing unlawful and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous.

952. Blackbaud acted intentionally, knowingly, and maliciously to violate Hawaii's Unfair Practices and Unfair Competition Act, and recklessly disregarded Plaintiff and Hawaii Subclass members' rights.

953. As a direct and proximate result of Blackbaud's deceptive acts and practices, Plaintiff and Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

954. Plaintiff and Hawaii Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, benefit of the bargain damages, treble damages, injunctive relief, and reasonable attorneys' fees and costs.

**COUNT 28: HAWAII UNIFORM DECEPTIVE TRADE PRACTICE ACT,
Haw. Rev. Stat. §§ 481A-3, *et seq.***

955. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges Paragraphs 1-954, as if fully alleged herein. This claim is brought individually under the laws of Hawaii and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practice.

956. Plaintiff and Hawaii Subclass members are “persons” as defined by Haw. Rev. Stat.

§ 481A-2.

957. Blackbaud engaged in unfair and deceptive trade practices in the conduct of its business, violating Haw. Rev. Stat. § 481A-3, including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised; and
- d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

958. Blackbaud’s unfair and deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Hawaii Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Hawaii Subclass members’ Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Hawaii Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Hawaii Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

959. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

960. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Hawaii Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Hawaii Subclass members into believing they did not need to take actions to secure their identities.

961. The above unfair and deceptive practices and acts by Blackbaud were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Hawaii Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

962. As a direct and proximate result of Blackbaud's unfair, unlawful, and deceptive trade practices, Plaintiff and Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

963. Plaintiff and Hawaii Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, attorneys' fees and costs, and any other relief that the Court deems proper.

CLAIMS ON BEHALF OF THE IDAHO SUBCLASS

COUNT 29: IDAHO CONSUMER PROTECTION ACT, Idaho Code §§ 48-601, *et seq.*

964. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Idaho Subclass, repeats and alleges Paragraphs 1-963, as if fully alleged herein. This claim is brought individually under the laws of Idaho and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

965. Blackbaud is a "person" as defined by Idaho Code § 48-602(1).

966. Blackbaud's conduct as alleged herein pertained to "goods" and "services" as defined by Idaho Code § 48-602(6) and (7).

967. Blackbaud advertised, offered, or sold goods or services in Idaho and engaged in trade or commerce directly or indirectly affecting the people of Idaho.

968. Blackbaud engaged in unfair and deceptive acts or practices, and unconscionable acts and practices, in the conduct of trade and commerce with respect to the sale and advertisement of goods and services, in violation of Idaho Code §§ 48-603 and 48-603(C), including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;
- b. Representing that goods are of a particular standard, quality, or grade when they are of another;
- c. Advertising goods or services with intent not to sell them as advertised;
- d. Engaging in other acts and practices that are otherwise misleading, false, or deceptive to consumers; and

- e. Engaging in unconscionable methods, acts or practices in the conduct of trade or commerce.
- f. Blackbaud's unfair, deceptive, and unconscionable acts and practices include:
- g. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Idaho Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- h. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- i. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Idaho Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- j. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Idaho Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- k. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Idaho Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- l. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Idaho Subclass members of the Data Breach;
- m. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- n. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Idaho Subclass members' Private Information; and
- o. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Idaho Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505.

969. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

970. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Idaho Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Idaho Subclass members into believing they did not need to take actions to secure their identities.

971. Blackbaud intended to mislead Plaintiff and Idaho Subclass members and induce them to rely on its misrepresentations and omissions. Blackbaud knew its representations and omissions were false.

972. Blackbaud acted intentionally, knowingly, and maliciously to violate Idaho's Consumer Protection Act, and recklessly disregarded Plaintiff and Idaho Subclass members' rights.

973. As a direct and proximate result of Blackbaud's unfair, deceptive, and unconscionable conduct, Plaintiff and Idaho Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

974. Plaintiff and Idaho Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, injunctive relief, costs, and attorneys' fees.

CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS

COUNT 30: ILLINOIS CONSUMER FRAUD ACT, 815 ILCS §§ 505, *et seq.*

975. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1-974, as if fully alleged herein. This claim is brought individually under the laws of Illinois and on behalf of all

other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud.

976. Blackbaud is a “person” as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

977. Plaintiff and Illinois Subclass members are “consumers” as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

978. Blackbaud’s conduct as described herein was in the conduct of “trade” or “commerce” as defined by 815 Ill. Comp. Stat. § 505/1(f).

979. Blackbaud’s deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat. § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Illinois Subclass members’ Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat. § 505/2RR,

- and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Illinois Subclass members of the Data Breach;
 - g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
 - h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Illinois Subclass members' Private Information; and
 - i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat. § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).
 - j. By failing to provide disclose the Data Breach in a timely fashion, in violation of 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*

980. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

981. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Illinois Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Illinois Subclass members into believing they did not need to take actions to secure their identities.

982. Blackbaud intended to mislead Plaintiff and Illinois Subclass members and induce them to rely on its misrepresentations and omissions.

983. The above unfair and deceptive practices and acts by Blackbaud offend public policy, and were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial

injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

984. Blackbaud acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff and Illinois Subclass members' rights.

985. As a direct and proximate result of Blackbaud's unfair, unlawful, and deceptive acts and practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

986. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

**COUNT 31: ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT,
815 ILCS §§ 510/2, *et seq.***

987. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1-986, as if fully alleged herein. This claim is brought individually under the laws of Illinois and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

988. Blackbaud is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

989. Blackbaud engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

- a. Representing that goods or services have characteristics that they do not have;

- b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;
 - c. Advertising goods or services with intent not to sell them as advertised; and
 - d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.
990. Blackbaud's deceptive trade practices include:
- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
 - b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
 - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat. § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;
 - d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Illinois Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
 - e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat. § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);
 - f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Illinois Subclass members of the Data Breach;

- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Illinois Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a)).

991. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

992. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Illinois Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Illinois Subclass members into believing they did not need to take actions to secure their identities.

993. The above unfair and deceptive practices and acts by Blackbaud were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

994. As a direct and proximate result of Blackbaud's unfair, unlawful, and deceptive trade practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial

accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

995. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

CLAIMS ON BEHALF OF THE INDIANA SUBCLASS

COUNT 32: INDIANA DECEPTIVE CONSUMER SALES ACT, Ind. Code §§ 24-5-0.5-1, *et seq.*

996. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Indiana Subclass, repeats and alleges Paragraphs 1-995, as if fully alleged herein. This claim is brought individually under the laws of Indiana and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive consumer sales.

997. Blackbaud is a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

998. Blackbaud is a "supplier" as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(3)(A).

999. Blackbaud engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

1000. Blackbaud's representations and omissions include both implicit and explicit representations.

1001. Blackbaud's unfair, abusive, and deceptive acts, omissions, and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Indiana Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a

- direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c), which was a direct and proximate cause of the Data Breach;
 - d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Indiana Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
 - e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c);
 - f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Indiana Subclass members of the Data Breach;
 - g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
 - h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Indiana Subclass members' Private Information; and
 - i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c).

1002. Blackbaud's acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1003. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Georgia Subclass members, that their

Private Information was not exposed and misled Plaintiffs and the Indiana Subclass members into believing they did not need to take actions to secure their identities.

1004. The injury to consumers from Blackbaud's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their Private Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1005. Consumers could not have reasonably avoided injury because Blackbaud's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Blackbaud created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1006. Blackbaud's inadequate data security had no countervailing benefit to consumers or to competition.

1007. Blackbaud's acts and practices were "abusive" for numerous reasons, including:

- a. Because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. Blackbaud's failure to disclose the inadequacies in its data security interfered with consumers' decision-making in a variety of their transactions.
- b. Because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in Blackbaud's data security, consumers lacked an understanding of the material risks and costs of a variety of their transactions.
- c. Because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and Blackbaud concerning the state of Blackbaud's security.
- d. Because Blackbaud took unreasonable advantage of consumers' reasonable reliance that it was acting in their interests to secure their data.

Consumers' reliance was reasonable for the reasons discussed four paragraphs below.

1008. Blackbaud also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

- a. Misrepresenting that the subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have;
- b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not;
- c. Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (*i.e.*, more data security) than the supplier intends or reasonably expects; and
- d. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

1009. Blackbaud intended to mislead Plaintiff and Indiana Subclass members and induce them to rely on its misrepresentations and omissions.

1010. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1011. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Indiana Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Indiana Subclass members into believing they did not need to take actions to secure their identities.

1012. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information

regarding millions of consumers, including Plaintiffs, the Class, and the Indiana Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Indiana Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1013. Blackbaud had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession. This duty arose because Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Indiana Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Indiana Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Indiana Subclass—and Blackbaud, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Blackbaud. Blackbaud's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Indiana Subclass that contradicted these representations.

1014. Blackbaud acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiff and Indiana Subclass members' rights. Blackbaud's actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, mere negligence, or other human failing.

1015. Plaintiff sent a demand for relief on behalf of the Indiana Subclass pursuant to Ind. Code § 24-5-0.5-5 on February 24, 2021. Blackbaud has not cured its unfair, abusive, and deceptive acts and practices, or its violations of Indiana Deceptive Consumer Sales Act were incurable.

1016. Since Plaintiff provided the requisite notice, Blackbaud has failed to cure its violations of the Indiana Deceptive Consumer Sales Act.

1017. Blackbaud's conduct includes incurable deceptive acts that Blackbaud engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5-2(a)(8).

1018. As a direct and proximate result of Blackbaud's uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiff and Indiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1019. Blackbaud's violations present a continuing risk to Plaintiff and Indiana Subclass members as well as to the general public.

1020. Plaintiff and Indiana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$500 for each non-willful violation; the

greater of treble damages or \$1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

CLAIMS ON BEHALF OF THE IOWA SUBCLASS

COUNT 33: PERSONAL INFORMATION SECURITY BREACH PROTECTION LAW, Iowa Code § 715C.2

1021. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Iowa Subclass, repeats and alleges Paragraphs 1-1020, as if fully alleged herein. This claim is brought individually under the laws of Iowa and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding security breach protection.

1022. Blackbaud is a business that owns or licenses computerized data that includes "Personal information" as defined by Iowa Code § 715C.2(1).

1023. Plaintiff and Iowa Subclass members' Private Information includes "Personal information" as covered under Iowa Code § 715C.2(1).

1024. Blackbaud is required to accurately notify Plaintiff and Iowa Subclass members if it becomes aware of a breach of its data security program in the most expeditious time possible and without unreasonable delay under Iowa Code § 715C.2(1).

1025. Because Blackbaud was aware of a breach of its security system, Blackbaud had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Iowa Code § 715C.2(1).

1026. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated Iowa Code § 715C.2(1).

1027. Pursuant to Iowa Code § 715C.2(9), a violation of Iowa Code § 715C.2(1) is an unlawful practice pursuant to Iowa Code Ann. § 714.16(7).

1028. As a direct and proximate result of Blackbaud's violations of Iowa Code § 715C.2(1), Plaintiff and Iowa Subclass members suffered damages, as described above.

1029. Plaintiff and Iowa Subclass members seek relief under Iowa Code § 714.16(7), including actual damages and injunctive relief.

**COUNT 34: IOWA PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT,
Iowa Code § 714H**

1030. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Iowa Subclass, repeats and alleges Paragraphs 1029, as if fully alleged herein. This claim is brought individually under the laws of Iowa and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud.

1031. Blackbaud is a "person" as defined by Iowa Code § 714H.2(7).

1032. Plaintiff and Iowa Subclass members are "consumers" as defined by Iowa Code § 714H.2(3).

1033. Blackbaud's conduct described herein related to the "sale" or "advertisement" of "merchandise" as defined by Iowa Code §§ 714H.2(2), (6), & (8).

1034. Blackbaud engaged in unfair, deceptive, and unconscionable trade practices, in violation of the Iowa Private Right of Action for Consumer Frauds Act, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Iowa Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Iowa Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45,

- HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Iowa Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
 - e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Iowa Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
 - f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Iowa Subclass members of the Data Breach;
 - g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
 - h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Iowa Subclass members' Private Information; and
 - i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Iowa Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1035. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1036. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Iowa Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Iowa Subclass members into believing they did not need to take actions to secure their identities.

1037. Blackbaud intended to mislead Plaintiff and Iowa Subclass members and induce them to rely on its misrepresentations and omissions.

1038. Blackbaud acted intentionally, knowingly, and maliciously to violate Iowa's Private Right of Action for Consumer Frauds Act, and recklessly disregarded Plaintiff and Iowa Subclass members' rights.

1039. As a direct and proximate result of Blackbaud's unfair, deceptive, and unconscionable conduct, Plaintiff and Iowa Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1040. Plaintiff has provided the requisite notice to the Iowa Attorney General, the office of which approved the filing of this Class action lawsuit pursuant to Iowa Code § 714H.7.

1041. Plaintiff and Iowa Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE KANSAS SUBCLASS

COUNT 35: PROTECTION OF CONSUMER INFORMATION, Kan. Stat. Ann. §§ 50-7a02(a), *et seq.*

1042. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeats and alleges Paragraphs 1-1041, as if fully alleged herein. This claim is brought individually under the laws of Kansas and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding protection of consumer information.

1043. Blackbaud is a business that owns or licenses computerized data that includes "personal information" as defined by Kan. Stat. Ann. § 50-7a02(a).

1044. Plaintiff and Kansas Subclass members' Private Information includes "personal information" as covered under Kan. Stat. Ann. § 50-7a02(a).

1045. Blackbaud is required to accurately notify Plaintiffs and Kansas Subclass members if it becomes aware of a breach of its data security program that was reasonably likely to have caused misuse of Plaintiff and Kansas Subclass members' Private Information, in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

1046. Because Blackbaud was aware of a breach of its security system that was reasonably likely to have caused misuse of Plaintiffs' and Kansas Subclass members' Private Information, Blackbaud had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

1047. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated Kan. Stat. Ann. § 50-7a02(a).

1048. As a direct and proximate result of Blackbaud's violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff and Kansas Subclass members suffered damages and will continue to suffer damages, as described above.

1049. Plaintiff and Kansas Subclass members seek relief under Kan. Stat. Ann. § 50-7a02(g), including equitable relief.

**COUNT 36: KANSAS CONSUMER PROTECTION ACT,
K.S.A. §§ 50-623, *et seq.***

1050. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeats and alleges Paragraphs 1-1049, as if fully alleged herein. This claim is brought individually under the laws of Kansas and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

1051. K.S.A. §§ 50-623, *et seq.* is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

1052. Plaintiff and Kansas Subclass members are “consumers” as defined by K.S.A. § 50-624(b).

1053. The acts and practices described herein are “consumer transactions,” as defined by K.S.A. § 50-624(c).

1054. Blackbaud is a “supplier” as defined by K.S.A. § 50-624(l).

1055. Blackbaud advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

1056. Blackbaud engaged in deceptive and unfair acts or practices, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Kansas Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Kansas’s identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Kansas Subclass members’ Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Kansas’s identity fraud statute, the Wayne Owen Act, K.S.A. §

50-6,139b;

- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Kansas Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Kansas Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b.

1057. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1058. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Kansas Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Kansas Subclass members into believing they did not need to take actions to secure their identities.

1059. Blackbaud intended to mislead Plaintiff and Kansas Subclass members and induce them to rely on its misrepresentations and omissions.

1060. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Kansas Subclass.

Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Kansas Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1061. Blackbaud also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including:

- a. Knowingly taking advantage of the inability of Plaintiff and the Kansas Subclass to reasonably protect their interests, due to their lack of knowledge (*see* K.S.A. § 50-627(b)(1)); and
- b. Requiring Plaintiff and the Kansas Subclass to enter into a consumer transaction on terms that Blackbaud knew were substantially one-sided in favor of Blackbaud (*see* K.S.A. § 50-627(b)(5)).

1062. Plaintiff and the Kansas Subclass had unequal bargaining power with respect to their ability to control the security and confidentiality of their Private Information in Blackbaud's possession.

1063. The above unfair, deceptive, and unconscionable practices and acts by Blackbaud were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

1064. Blackbaud acted intentionally, knowingly, and maliciously to violate Kansas's Consumer Protection Act, and recklessly disregarded Plaintiff and Kansas Subclass members' rights.

1065. As a direct and proximate result of Blackbaud's unfair, deceptive, and unconscionable trade practices, Plaintiff and Kansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-

monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1066. Plaintiff and Kansas Subclass members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE KENTUCKY SUBCLASS

COUNT 37: KENTUCKY COMPUTER SECURITY BREACH NOTIFICATION ACT, Ky. Rev. Stat. Ann. §§ 365.732, *et seq.*

1067. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeats and alleges Paragraphs 1-1066, as if fully alleged herein. This claim is brought individually under the laws of Kentucky and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding security breach notification.

1068. Blackbaud is required to accurately notify Plaintiff and Kentucky Subclass members if it becomes aware of a breach of its data security program that was reasonably likely to have caused unauthorized persons to acquire Plaintiff and Kentucky Subclass members' Private Information, in the most expedient time possible and without unreasonable delay under Ky. Rev. Stat. Ann. § 365.732(2).

1069. Blackbaud is a business that holds computerized data that includes "personal information" as defined by Ky. Rev. Stat. Ann. § 365.732(2).

1070. Plaintiff and Kentucky Subclass members' Private Information includes "personal information" as covered under Ky. Rev. Stat. Ann. § 365.732(2).

1071. Because Blackbaud was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff and Kentucky Subclass members' Private Information, Blackbaud had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ky. Rev. Stat. Ann. § 365.732(2).

1072. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated Ky. Rev. Stat. Ann. § 365.732(2).

1073. Ky. Rev. Stat. Ann. §§ 365.732 *et seq.* provides no inclusive civil remedy.

1074. Plaintiff and Kentucky Subclass members are within the Class of persons Ky. Rev. Stat. Ann. §§365.732 *et seq.* is designed to protect.

1075. As a direct and proximate result of Blackbaud's violations of Ky. Rev. Stat. Ann. § 365.732(2), Plaintiff and Kentucky Subclass members suffered damages, as described above.

1076. Plaintiff and Kentucky Subclass members seek relief under Ky. Rev. Stat. Ann. § 446.070, including actual damages.

**COUNT 38: KENTUCKY CONSUMER PROTECTION ACT,
Ky. Rev. Stat. §§ 367.110, *et seq.***

1077. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeats and alleges Paragraphs 1-1076, as if fully alleged herein. This claim is brought individually under the laws of Kentucky and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

1078. Blackbaud is a "person" as defined by Ky. Rev. Stat. § 367.110(1).

1079. Blackbaud advertised, offered, or sold goods or services in Kentucky and engaged in trade or commerce directly or indirectly affecting the people of Kentucky, as defined by Ky. Rev. Stat. 367.110(2).

1080. Blackbaud engaged in unfair, false, misleading, deceptive, and unconscionable acts or practices, in violation of Ky. Rev. Stat. § 367.170, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Kentucky Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Kentucky Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Kentucky Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Kentucky Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505.

1081. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1082. Blackbaud made these representations for the benefit of Plaintiffs and Kentucky Subclass members.

1083. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Kentucky Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Kentucky Subclass members into believing they did not need to take actions to secure their identities.

1084. Blackbaud intended to mislead Plaintiff and Kentucky Subclass members and induce them to rely on its misrepresentations and omissions.

1085. Plaintiff and Kentucky Subclass members' purchased goods or services for personal, family, or household purposes and suffered ascertainable losses of money or property as a result of Blackbaud's unlawful acts and practices.

1086. The above unlawful acts and practices by Blackbaud were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

1087. Blackbaud acted intentionally, knowingly, and maliciously to violate Kentucky's Consumer Protection Act, and recklessly disregarded Plaintiff and Kentucky Subclass members' rights.

1088. As a direct and proximate result of Blackbaud's unlawful acts and practices, Plaintiff and Kentucky Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for

fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1089. Plaintiff and Kentucky Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution or other equitable relief, injunctive relief, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE LOUISIANA SUBCLASS

COUNT 39: DATABASE SECURITY BREACH NOTIFICATION LAW, La. Rev. Stat. Ann. §§ 51:3074(A), *et seq.*

1090. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and alleges Paragraphs 1-1089, as if fully alleged herein. This claim is brought individually under the laws of Louisiana and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding security breach notification.

1091. Blackbaud is a business that owns or licenses computerized data that includes "personal information" as defined by La. Rev. Stat. Ann. § 51:3074(C).

1092. Plaintiff and Louisiana Subclass members' Private Information includes "personal information" as covered under La. Rev. Stat. Ann. § 51:3074(C).

1093. Blackbaud is required to accurately notify Plaintiff and Louisiana Subclass members if it becomes aware of a breach of its data security program that was reasonably likely to have caused unauthorized persons to acquire Plaintiff and Louisiana Subclass members' Private Information, in the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. § 51:3074(C).

1094. Because Blackbaud was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff and Louisiana Subclass

members' Private Information, Blackbaud had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(C).

1095. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated La. Rev. Stat. Ann. § 51:3074(C).

1096. As a direct and proximate result of Blackbaud's violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiff and Louisiana Subclass members suffered damages and will continue to suffer damages, as described above.

1097. Plaintiff and Louisiana Subclass members seek relief under La. Rev. Stat. Ann. § 51:3075, including actual damages.

COUNT 40: LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, La. Rev. Stat. Ann. §§ 51:1401, *et seq.*

1098. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually repeats and alleges Paragraphs 1-1097, as if fully alleged herein. This claim is brought individually under the laws of Louisiana.

1099. Blackbaud and Plaintiff are "persons" within the meaning of the La. Rev. Stat. Ann. § 51:1402(8).

1100. Plaintiff is a "consumer" within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

1101. Blackbaud engaged in "trade" or "commerce" within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

1102. The Louisiana Unfair Trade Practices and Consumer Protection Law ("Louisiana CPL") makes unlawful "unfair or deceptive acts or practices in the conduct of any trade or commerce." La. Rev. Stat. Ann. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

1103. Blackbaud participated in unfair and deceptive acts and practices that violated the Louisiana CPL, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Louisiana Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Louisiana Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Louisiana Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Louisiana Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

j. Failing to disclose the Data Breach in a timely and accurate manner in violation of La. Rev. Stat. Ann. §51:3074.

1104. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1105. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs, that their Private Information was not exposed and misled Plaintiffs and the Louisiana Subclass members into believing they did not need to take actions to secure their identities.

1106. Blackbaud intended to mislead Plaintiff and induce them to rely on its misrepresentations and omissions.

1107. Blackbaud's unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

1108. Blackbaud acted intentionally, knowingly, and maliciously to violate Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff's rights.

1109. Had Blackbaud disclosed to Plaintiffs that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Louisiana Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a

secure platform for Private Information data, Plaintiffs acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1110. As a direct and proximate result of Blackbaud's unfair and deceptive acts and practices, Plaintiffs have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1111. Plaintiff seeks all monetary and non-monetary relief allowed by law, including actual damages; treble damages for Blackbaud's knowing violations of the Louisiana CPL; declaratory relief; attorneys' fees; and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE MAINE SUBCLASS

COUNT 41: MAINE UNFAIR TRADE PRACTICES ACT, 5 Me. Rev. Stat. §§ 205, 213, *et seq.*

1112. The Maine Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maine Subclass, repeats and alleges Paragraphs 1-1111, as if fully alleged herein. This claim is brought individually under the laws of Maine and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair trade practices.

1113. Blackbaud is a "person" as defined by 5 Me. Stat. § 206(2).

1114. Blackbaud's conduct as alleged herein related was in the course of "trade and commerce" as defined by 5 Me. Stat. § 206(3).

1115. Plaintiff and Maine Subclass members purchased goods and/or services for personal, family, and/or household purposes.

1116. Plaintiff sent a demand for relief on behalf of the Maine Subclass pursuant to 5 Me. Rev. Stat. § 213(1-A) on February 24, 2021.

1117. Blackbaud engaged in unfair and deceptive trade acts and practices in the conduct of trade or commerce, in violation of 5 Me. Rev. Stat. §207, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Maine Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Maine Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Maine Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maine Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42

U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1118. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1119. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Maine Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Maine Subclass members into believing they did not need to take actions to secure their identities.

1120. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Maine Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Maine Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1121. As a direct and proximate result of Blackbaud's unfair and deceptive acts and conduct, Plaintiff and Maine Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for

fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1122. Plaintiff and the Maine Subclass members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive and other equitable relief, and attorneys' fees and costs.

**COUNT 42: MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT,
10 Me. Rev. Stat. §§ 1212, *et seq.***

1123. The Maine Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maine Subclass, repeats and alleges Paragraphs 1-1122, as if fully alleged herein. This claim is brought individually under the laws of Maine and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

1124. Blackbaud is a "person" as defined by 10 Me. Rev. Stat. § 1211(5).

1125. Blackbaud advertised, offered, or sold goods or services in Maine and engaged in trade or commerce directly or indirectly affecting the people of Maine.

1126. Blackbaud engaged in deceptive trade practices in the conduct of its business, in violation of 10 Me. Rev. Stat. §1212, including:

- a. Representing that goods or services have characteristics that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;
- c. Advertising goods or services with intent not to sell them as advertised; and
- d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

1127. Blackbaud's deceptive trade practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Maine Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Maine Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Maine Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maine Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1128. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1129. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Maine Subclass members, that their

Private Information was not exposed and misled Plaintiffs and the Maine Subclass members into believing they did not need to take actions to secure their identities.

1130. Blackbaud intended to mislead Plaintiff and Maine Subclass members and induce them to rely on its misrepresentations and omissions.

1131. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Maine Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Maine Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1132. As a direct and proximate result of Blackbaud's deceptive trade practices, Plaintiff and Maine Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1133. Maine Subclass members are likely to be damaged by Blackbaud's ongoing deceptive trade practices.

1134. Plaintiff and the Maine Subclass members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive or other equitable relief, and attorneys' fees and costs.

**COUNT 43: MAINE CONFIDENTIALITY OF HEALTH CARE INFORMATION LAW,
22 M.R.S. § 1711-C**

1135. The Maine Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maine PHI Subclass, repeats and alleges Paragraphs 1-1134, as if fully alleged herein. This claim is brought individually under the laws of Maine and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding the confidentiality of health care information.

1136. The Maine Confidentiality of Health Care Information law prohibits, among other things, unauthorized disclosure of patient health care records. 22 M.R.S. § 1711-C (2).

1137. Plaintiff provided his PHI to a Social Good Entity which is a "health care practitioner" as defined by 22 M.R.S. § 1711-C (1)(F).

1138. Blackbaud is an "agent" of the Social Good Entity to which Plaintiff provided his PHI and is therefore a "health care practitioner" as defined by 22 M.R.S. § 1711-C (1)(F).

1139. Plaintiff is an "individual" whose health care information was disclosed without proper authorization as defined by 22 M.R.S. § 1711-C (1)(G).

1140. Blackbaud had a duty to develop and implement policies, standards and procedures to protect the confidentiality, security and integrity of the Plaintiff and the Maine PHI Subclass member's health care information to ensure that information is not negligently, inappropriately or unlawfully disclosed. 22 M.R.S. § 1711-C (7).

1141. Blackbaud disclosed health care information pertaining to the Plaintiff and the Maine PHI Subclass without their consent and for no other reason permitted by 22 M.R.S. § 1711-C.

1142. Unauthorized disclosure of health care information to hackers resulted from the affirmative actions of Blackbaud in maintaining the security of its computer system at levels that did not protect the confidentiality, security and integrity of the Plaintiff and the Maine Subclass member's health care information and allowed hackers to improperly access and copy private health care information of the Plaintiff and the Maine Subclass.

1143. The affirmative actions of Blackbaud in maintaining the security of its computer system at levels that allowed hackers to improperly access and copy private health care information of the Plaintiff and the Maine PHI Subclass. Blackbaud actively and affirmatively allowed the hackers to see and obtain the health care information of the Plaintiff and members of the Maine Subclass.

1144. Plaintiff and the Maine PHI Subclass members were injured and have suffered damages from Blackbaud's illegal disclosure and release of their health care information in violation of 22 M.R.S. § 1711-C (2).

1145. Plaintiff individual and on behalf of the Maine PHI Subclass seeks relief including but not limited to actual damages, injunctive relief, and/or attorneys' fees and costs under 22 M.R.S. § 1711-C (13)(B).

CLAIMS ON BEHALF OF THE MARYLAND SUBCLASS

COUNT 44: MARYLAND CONSUMER PROTECTION ACT, Md. Comm. Code §§ 13-301, *et seq.*

1146. The Maryland Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maryland Subclass, repeats and alleges Paragraphs 1-1145, as if

fully alleged herein. This claim is brought individually under the laws of Maryland and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

1147. Blackbaud is a person as defined by Md. Comm. Code § 13-101(h).

1148. Blackbaud's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Comm. Code § 13-101(i) and § 13-303.

1149. Maryland Subclass members are "consumers" as defined by Md. Comm. Code § 13-101(c).

1150. Blackbaud' advertises, offers, or sell "consumer goods" or "consumer services" as defined by Md. Comm. Code § 13-101(d).

1151. Blackbaud advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

1152. Blackbaud engaged in unfair and deceptive trade practices, in violation of Md. Comm. Code § 13-301, including:

- a. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;
- b. Representing that consumer goods or services have a characteristic that they do not have;
- c. Representing that consumer goods or services are of a particular standard, quality, or grade that they are not;
- d. Failing to state a material fact where the failure deceives or tends to deceive;
- e. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;
- f. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with

respect to an agreement, sale lease or rental.

1153. Blackbaud engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services, in violation of Md. Comm. Code § 13-303, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Maryland Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maryland Subclass members' Private Information, including duties imposed by FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Maryland Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maryland Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Maryland Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maryland Subclass members' Private Information; and

- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maryland Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503.
- j. Failing to take reasonable steps to protect against the unauthorized access or use of the personal information belonging to Plaintiff and Maryland Subclass members in violation of the Maryland Personal Information Protection Act, Md. Comm. Code §§14-3501 *et seq.*
- k. Publicly posting or displaying Social Security numbers belonging to the Plaintiff and Maryland Subclass members in violation of the Social Security Number Privacy Act, Md. Comm. Code §14-3401 *et. seq.*

1154. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information. Blackbaud's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

1155. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Maryland Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Maryland Subclass members into believing they did not need to take actions to secure their identities.

1156. Blackbaud intended to mislead Plaintiff and Maryland Subclass members and induce them to rely on its misrepresentations and omissions.

1157. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information

regarding millions of consumers, including Plaintiffs, the Class, and the Maryland Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Maryland Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1158. Blackbaud acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiff and Maryland Subclass members' rights.

1159. As a direct and proximate result of Blackbaud's unfair and deceptive acts and practices, Plaintiff and Maryland Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1160. Plaintiff and Maryland Subclass members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

**COUNT 45: MARYLAND CONFIDENTIALITY OF MEDICAL RECORDS ACT,
Md. Health-Gen. Code § 4-301, *et seq.***

1161. The Maryland Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maryland PHI Subclass, repeats and alleges Paragraphs 1-1160, as if fully alleged herein. This claim is brought individually under the laws of Maryland and on behalf of all other natural persons whose Private Information was compromised as a result of the

Data Breach and reside in states having similar laws regarding the confidentiality of medical records.

1162. The Maryland Confidentiality of Medical Record Act (“MCMRA”) prohibits, among other things, unauthorized disclosure of private medical records. Md. Code Health-Gen. § 4-302(a).

1163. Plaintiff provided her PHI to a Social Good Entity which is a “health care provider” as defined by Md. Code Health-Gen. § 4-301(g)(1).

1164. Blackbaud is an “agent” of the Social Good Entity to which Plaintiff provided her PHI and therefore is a health care provider as defined by Md. Code Health-Gen. § 4-301(g)(1).

1165. Blackbaud is also “person” to whom medical records are disclosed as defined by MD Code Health-Gen. § 4-302, and therefore subject to the requirements of the MCMRA.

1166. Plaintiff [] is a “patient”, as defined by Md. Code Ann., Health-Gen. § 4-301(k), of the Social Good Entity to which she provided her PHI.

1167. Blackbaud stored on its computer system “medical records” as defined by Md. Code Health-Gen. § 4-301(h)(i)(1) pertaining to the Plaintiff and the Maryland PHI Subclass.

1168. Blackbaud disclosed medical records pertaining to the Plaintiff and the Maryland PHI Subclass without their authorization and for no other reason permitted by Md. Code Health-Gen. § 4-302, and therefore violated Md. Code Health-Gen. § 4-302.

1169. Disclosure of medical records to unauthorized individuals resulted from the affirmative actions of Blackbaud in maintaining the security of its computer system at levels that allowed hackers to improperly access and copy private medical records of the Plaintiff and the Maryland PHI Subclass.

1170. Blackbaud's unauthorized disclosure of medical records has caused injury to the Plaintiff and the Maryland PHI Subclass.

1171. The Plaintiff and the Maryland PHI Subclass seek relief pursuant to Md. Code Health-Gen. § 4-309, including actual damages for Blackbaud's knowing violations of Md. Code Health-Gen. § 4-302.

CLAIMS ON BEHALF OF THE MASSACHUSETTS SUBCLASS

COUNT 46: MASSACHUSETTS CONSUMER PROTECTION ACT, Mass. Gen. Laws Ann. Ch. 93A, §§ 1, *et seq.*

1172. The Massachusetts Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Massachusetts Subclass, repeats and alleges Paragraphs 1-1171, as if fully alleged herein. This claim is brought individually under the laws of Massachusetts and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

1173. Blackbaud and Massachusetts Subclass members are "persons" as meant by Mass. Gen. Laws. Ann. Ch. 93A, § 1(a).

1174. Blackbaud operates in "trade or commerce" as meant by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

1175. Blackbaud advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

1176. Plaintiff sent a demand for relief on behalf of the Massachusetts Subclass pursuant to Mass. Gen. Laws Ann. Ch. 93A § 9(3) on February 24, 2021.

1177. Blackbaud engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A, § 2(a), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Massachusetts Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Massachusetts Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Massachusetts Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Massachusetts Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Massachusetts Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Massachusetts Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Massachusetts Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the

Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

1178. Blackbaud's acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that Blackbaud solely held the true facts about its inadequate security for Private Information, which Plaintiff and the Massachusetts Subclass members could not independently discover.

1179. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Massachusetts Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Massachusetts Subclass members into believing they did not need to take actions to secure their identities.

1180. Consumers could not have reasonably avoided injury because Blackbaud's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Blackbaud created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1181. Blackbaud's inadequate data security had no countervailing benefit to consumers or to competition.

1182. Blackbaud intended to mislead Plaintiff and Massachusetts Subclass members and induce them to rely on its misrepresentations and omissions. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1183. Blackbaud acted intentionally, knowingly, and maliciously to violate Massachusetts's Consumer Protection Act, and recklessly disregarded Plaintiff and Massachusetts Subclass members' rights.

1184. As a direct and proximate result of Blackbaud's unfair and deceptive, Plaintiff and Massachusetts Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1185. Plaintiff and Massachusetts Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, injunctive or other equitable relief, and attorneys' fees and costs.

**COUNT 47: MASSACHUSETTS RIGHT TO PRIVACY LAW,
Mass. Gen. Laws Ch. 214, § 1B**

1186. The Massachusetts Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota PHI Subclass, repeats and alleges Paragraphs 1-1185, as if fully alleged herein. This claim is brought individually under the laws of Massachusetts and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding the right to privacy.

1187. Massachusetts law recognizes the personal right to privacy and the right to enforce one's right to privacy. *See Mass. Gen. Laws Ch. 214, § 1B.*

1188. The right to privacy under Massachusetts law extends to medical records and information.

1189. At all relevant times, Plaintiff was a patient of the Social Good Entity, a healthcare provider, to which Plaintiff provided her PHI.

1190. At all relevant times, Blackbaud, an agent of the Social Good Entity to which Plaintiff provided her PHI, stored confidential PHI related to the Plaintiff and other Massachusetts PHI Subclass members on Blackbaud's computer system.

1191. Plaintiff and the Massachusetts PHI Subclass members did not authorize Blackbaud to disclose their personal health records and information to third parties.

1192. As described throughout this Complaint, Blackbaud negligently or intentionally disclosed and released Plaintiff and the Massachusetts PHI Subclass member's health care records and information inasmuch as it did not implement adequate security protocols to prevent unauthorized access to health care records, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data breach or otherwise comply with HIPAA data security requirements.

1193. As a direct and proximate result of Blackbaud's negligent or intentional acts, it disclosed and released Plaintiff and the Massachusetts PHI Subclass member's health care records to third parties without consent or authorization and caused injury to the Plaintiff and the Massachusetts PHI Subclass.

1194. Blackbaud's unauthorized disclosure of medical records and information has caused injury to the Plaintiff and the Massachusetts PHI Subclass.

1195. Accordingly, Plaintiff, individually and on behalf of members of the Massachusetts PHI Subclass, seek compensatory damages plus costs and attorney fees. *See* Mass. Gen. Laws Ch. 214, § 1B.

CLAIMS ON BEHALF OF THE MICHIGAN SUBCLASS

COUNT 48: MICHIGAN IDENTITY THEFT PROTECTION ACT, Mich. Comp. Laws Ann. §§ 445.72, *et seq.*

1196. The Michigan Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Michigan Subclass, repeats and alleges Paragraphs 1-1195, as if fully alleged herein. This claim is brought individually under the laws of Michigan and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding identity theft protection.

1197. Blackbaud is a business that owns or licenses computerized data that includes “personal information” as defined by Mich. Comp. Laws Ann. § 445.72(1).

1198. Plaintiff and Michigan Subclass members’ Private Information includes “personal information” as covered under Mich. Comp. Laws Ann. § 445.72(1).

1199. Blackbaud is required to accurately notify Plaintiff and Michigan Subclass members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

1200. Because Blackbaud discovered a security breach and had notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), Blackbaud had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

1201. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated Mich. Comp. Laws Ann. § 445.72(4).

1202. As a direct and proximate result of Blackbaud's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Michigan Subclass members suffered damages and will continue to suffer damages, as described above.

1203. Plaintiff and Michigan Subclass members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

**COUNT 49: MICHIGAN CONSUMER PROTECTION ACT,
Mich. Comp. Laws Ann. §§ 445.903, *et seq.***

1204. The Michigan Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Michigan Subclass, repeats and alleges Paragraphs 1-1203, as if fully alleged herein. This claim is brought individually under the laws of Michigan and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

1205. Blackbaud and Michigan Subclass members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

1206. Blackbaud advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

1207. Blackbaud engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

- a. Representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);
- b. Representing that its goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);
- c. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of

affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and

- d. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).
- e. Blackbaud's unfair, unconscionable, and deceptive practices include:
- f. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Michigan Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- g. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- h. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- i. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Michigan Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- j. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- k. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Michigan Subclass members of the Data Breach;
- l. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- m. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Michigan Subclass members' Private Information; and
- n. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and

privacy of Plaintiff and Michigan Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 1681e, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1208. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1209. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Michigan Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Michigan Subclass members into believing they did not need to take actions to secure their identities.

1210. Blackbaud intended to mislead Plaintiff and Michigan Subclass members and induce them to rely on its misrepresentations and omissions.

1211. Blackbaud acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff and Michigan Subclass members' rights.

1212. As a direct and proximate result of Blackbaud's unfair, unconscionable, and deceptive practices, Plaintiff and Michigan Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1213. Plaintiff and Michigan Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$250, injunctive relief, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE MINNESOTA SUBCLASS

COUNT 50: MINNESOTA CONSUMER FRAUD ACT, Minn. Stat. §§ 325F.68, *et seq.* and Minn. Stat. §§ 8.31, *et seq.*

1214. The Minnesota Plaintiff(s) identified above (“Plaintiffs,” for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and alleges Paragraphs 1-1213, as if fully alleged herein. This claim is brought individually under the laws of Minnesota and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud.

1215. Blackbaud, Plaintiffs, and members of the Minnesota Subclass are each a “person” as defined by Minn. Stat. § 325F.68(3).

1216. Blackbaud’s goods, services, commodities, and intangibles are “merchandise” as defined by Minn. Stat. § 325F.68(2).

1217. Blackbaud engaged in “sales” as defined by Minn. Stat. § 325F.68(4).

1218. Blackbaud, as the guardian and gatekeeper of Plaintiffs and Minnesota Subclass members’ Private Information, had special knowledge of material facts to which Plaintiffs, Minnesota Subclass members, and Social Good Entities did not.

1219. These material facts included, *inter alia*, that Blackbaud’s systems and networks were vulnerable to unauthorized access and exfiltration, and therefore, Plaintiffs and Minnesota Subclass members’ Private Information was vulnerable to being exposed, exfiltrated, and misused as a result of a Data Breach.

1220. Further, Blackbaud had special knowledge once the Data Breach occurred of material facts to which Plaintiffs, Minnesota Subclass members, and Social Good Entities did not. This special knowledge was due to Blackbaud’s discovery of the cyberattack and subsequent

forensic investigation into what Private Information was exposed, that Plaintiffs, Minnesota Subclass members, and Social Good Entities did not have access too.

1221. These material facts included, *inter alia*, that Plaintiffs and Subclass members' Private Information was accessed and infiltrated.

1222. Despite holding such special knowledge, Blackbaud failed to disclose these material facts to Plaintiffs, Minnesota Subclass members and Social Good Entities to enable them to decide whether to entrust Private Information to Blackbaud or for Plaintiffs and Minnesota Subclass members to take appropriate actions to secure their identities.

1223. Blackbaud further engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise, in violation of Minn. Stat. § 325F.69(1), including:

1224. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Minnesota Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

- a. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Minnesota Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Minnesota Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- d. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Minnesota Subclass members' Private Information, including duties imposed by the FTC Act,

15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

- e. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Minnesota Subclass members of the Data Breach;
- f. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Minnesota Subclass members' Private Information; and
- h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Minnesota Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1225. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1226. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Minnesota Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Minnesota Subclass members into believing they did not need to take actions to secure their identities.

1227. Blackbaud intended to mislead Plaintiffs and Minnesota Subclass members and induce them to rely on its misrepresentations and omissions.

1228. Blackbaud's fraudulent, misleading, and deceptive practices affected the public interest, including millions of Minnesotans affected by the Data Breach.

1229. As a direct and proximate result of Blackbaud's fraudulent, misleading, and deceptive practices, Plaintiffs and Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary

damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1230. Plaintiffs and Minnesota Subclass members seek injunctive relief requiring Blackbaud to adequately protect Plaintiffs and Minnesota Subclass members' Private Information from future cyber attacks, and to require that Blackbaud provide Plaintiffs and Minnesota Subclass members with sufficient resources to safeguard their identities related to the risks arising from the Data Breach at issue.

1231. Such remedies would provide a public benefit aimed at altering Blackbaud's conduct, protecting Plaintiffs and Minnesota Subclass members' Private Information, and providing resources for continued, future efforts of safeguarding their identities related to the risks arising from the Data Breach at issue.

1232. Plaintiffs and Minnesota Subclass members further seek all monetary and non-monetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

**COUNT 51: MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT,
Minn. Stat. §§ 325D.43, *et seq.***

1233. The Minnesota Plaintiff(s) identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and alleges Paragraphs 1-1232, as if fully alleged herein. This claim is brought individually under the laws of Minnesota and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

1234. By engaging in deceptive trade practices in the course of its business and vocation, directly or indirectly affecting the people of Minnesota, Blackbaud violated Minn. Stat. § 325D.44, including the following provisions:

- a. Representing that its goods and services had characteristics, uses, and benefits that they did not have, in violation of Minn. Stat. § 325D.44(1)(5);
- b. Representing that goods and services are of a particular standard or quality when they are of another, in violation of Minn. Stat. § 325D.44(1)(7);
- c. Advertising goods and services with intent not to sell them as advertised, in violation of Minn. Stat. § 325D.44(1)(9); and
- d. Engaging in other conduct which similarly creates a likelihood of confusion or misunderstanding, in violation of Minn. Stat. § 325D.44(1)(13).
- e. Blackbaud's deceptive practices include:
- f. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Minnesota Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- g. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- h. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Minnesota Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- i. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Minnesota Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- j. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Minnesota Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;

- k. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Minnesota Subclass members of the Data Breach;
- l. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- m. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Minnesota Subclass members' Private Information; and
- n. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Minnesota Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1235. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1236. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Minnesota Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Minnesota Subclass members into believing they did not need to take actions to secure their identities.

1237. Blackbaud intended to mislead Plaintiffs and Minnesota Subclass members and induce them to rely on its misrepresentations and omissions.

1238. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Minnesota Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate

state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Minnesota Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1239. Blackbaud acted intentionally, knowingly, and maliciously to violate Minnesota's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs and Minnesota Subclass members' rights.

1240. Plaintiffs and Minnesota Subclass members are likely to be damaged in the future given that Blackbaud still maintains their Private Information, continues to adequately safeguard and protect this information from unauthorized access in the future, and therefore, has created a likelihood that such information may be exposed during a future Data Breach.

1241. As a direct and proximate result of Blackbaud's deceptive trade practices, Plaintiffs and Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1242. Plaintiffs and Minnesota Subclass members seek injunctive relief requiring Blackbaud to adequately protect Plaintiffs and Minnesota Subclass members' Private Information from future cyber attacks, and to require that Blackbaud provide Plaintiffs and Minnesota Subclass members with sufficient resources to safeguard their identities related to the risks arising from the Data Breach at issue.

1243. Such remedies would provide a public benefit aimed at altering Blackbaud's conduct, protecting Plaintiffs and Minnesota Subclass members' Private Information, and providing resources for continued, future efforts of safeguarding their identities related to the risks arising from the Data Breach at issue.

1244. Plaintiffs and Minnesota Subclass members further seek all monetary and non-monetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

**COUNT 52: MINNESOTA HEALTH RECORDS ACT,
Minn. Stat. § 144.291, *et seq.***

1245. The Minnesota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota PHI Subclass, repeats and alleges Paragraphs 1-1244, as if fully alleged herein. This claim is brought individually under the laws of Minnesota and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding health records.

1246. At all relevant times, Plaintiff was a "patient" of a Social Good Entity (to which she provided her PHI) which is a "provider", as those terms are construed under the Minnesota Health Records Act. *See* Minn. Stat. § 144.291, Subd. 2(g) and (i).

1247. At all times relevant to this action, Blackbaud stored "health care records" of the Plaintiff and other Minnesota PHI Subclass members as those terms are construed under the Minnesota Health Records Act in connection with the operation of the Social Good Entity and/or its philanthropic foundations. *See* Minn. Stat. § 144.291, Subd. 2(c).

1248. Absent an applicable exception under the statute or other law, the Minnesota Health Records Act makes it unlawful for someone, such as Blackbaud, who receives records from a

provider to release a patient's health care records to a third party without the patient's signed and dated consent. *See* Minn. Stat. § 144.293, Subd. 2 and 5.

1249. None of the exceptions to the requirement to obtain a patient's consent to release health care records are applicable to Blackbaud's release of health care records at issue here. *See* Minn. Stat. § 144.293, Subd. 5.

1250. Plaintiff and other Minnesota PHI Subclass members did not provide consent to release their health care records to third parties.

1251. Blackbaud negligently or intentionally disclosed and released Plaintiff and the Minnesota PHI Subclass members' health care records inasmuch as it did not implement adequate security protocols to prevent unauthorized access to health care records, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data breach or otherwise comply with HIPAA data security requirements.

1252. As a direct and proximate result of Blackbaud's negligent or intentional acts, it disclosed and released Plaintiff's health care records to third parties without the Plaintiff's consent and caused injury to the Plaintiff and the Minnesota PHI Subclass.

1253. Blackbaud's unauthorized disclosure of medical records has caused injury to the Plaintiff and the Minnesota PHI Subclass.

1254. Accordingly, Plaintiff, individually and on behalf of members of the Minnesota PHI Subclass, seek compensatory damages plus costs and attorney fees. *See* Minn. Stat. § 144.298.

CLAIMS ON BEHALF OF THE MISSISSIPPI SUBCLASS

COUNT 53: MISSISSIPPI CONSUMER PROTECTION ACT, Miss. Code §§ 75-24-1, *et seq.*

1255. The Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Mississippi Subclass, repeats and alleges Paragraphs 1-1254, as if fully alleged herein. This claim is brought individually under the laws of Mississippi and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

1256. Blackbaud is a “person,” as defined by Miss. Code § 75-24-3.

1257. Blackbaud advertised, offered, or sold goods or services in Mississippi and engaged in trade or commerce directly or indirectly affecting the people of Mississippi, as defined by Miss. Code § 75-24-3.

1258. Plaintiff has complied with all pre-conditions for bringing a private action under Miss. Code § 75-24-15.

1259. Blackbaud engaged in unfair and deceptive trade acts or practices, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Mississippi Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Mississippi Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Mississippi Subclass members’ Private Information, including

by implementing and maintaining reasonable security measures;

- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Mississippi Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Mississippi Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Mississippi Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Mississippi Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1260. The above-described conduct violated Miss. Code Ann. § 75-24-5(2), including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;
- b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and
- c. Advertising goods or services with intent not to sell them as advertised.

1261. Blackbaud intended to mislead Plaintiff and Mississippi Subclass members and induce them to rely on its misrepresentations and omissions.

1262. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1263. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Mississippi Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Mississippi Subclass members into believing they did not need to take actions to secure their identities.

1264. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Mississippi Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Mississippi Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1265. Blackbaud had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted professional standards in its industry, and the position of trust described in the immediately-preceding paragraph. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Mississippi Subclass—and Blackbaud, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Blackbaud. Blackbaud's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Mississippi Subclass that contradicted these representations.

1266. Blackbaud acted intentionally, knowingly, and maliciously to violate Mississippi's Consumer Protection Act, and recklessly disregarded Plaintiff and Mississippi Subclass members' rights.

1267. As a direct and proximate result of Blackbaud's unfair and deceptive acts or practices and Plaintiff and Mississippi Subclass members' purchase of goods or services primarily for personal, family, or household purposes, Plaintiff and Mississippi Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1268. Blackbaud's violations present a continuing risk to Plaintiff and Mississippi Subclass members as well as to the general public.

1269. Plaintiff and Mississippi Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution and other relief under Miss. Code § 75-24-11, injunctive relief, punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MISSOURI SUBCLASS

COUNT 54: MISSOURI MERCHANDISE PRACTICES ACT, Mo. Rev. Stat. §§ 407.010, *et seq.*

1270. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Missouri Subclass, repeats and alleges Paragraphs 1-1269, as if fully alleged herein. This claim is brought individually under the laws of Mississippi and on behalf

of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding merchandise practices.

1271. Blackbaud is a “person” as defined by Mo. Rev. Stat. § 407.010(5).

1272. Blackbaud advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(4), (6) and (7).

1273. Plaintiff and Missouri Subclass members purchased or leased goods or services primarily for personal, family, or household purposes.

1274. Blackbaud engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Missouri Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Missouri Subclass members’ Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§

6501-6505;

- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Missouri Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Missouri Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1275. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1276. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Missouri Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Missouri Subclass members into believing they did not need to take actions to secure their identities.

1277. Blackbaud intended to mislead Plaintiff and Missouri Subclass members and induce them to rely on its misrepresentations and omissions.

1278. Blackbaud acted intentionally, knowingly, and maliciously to violate Missouri's Merchandise Practices Act, and recklessly disregarded Plaintiff and Missouri Subclass members' rights.

1279. As a direct and proximate result of Blackbaud's unlawful, unfair, and deceptive acts and practices, Plaintiff and Missouri Subclass members have suffered and will continue to

suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1280. Plaintiff and Missouri Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

CLAIMS ON BEHALF OF THE MONTANA SUBCLASS

COUNT 55: COMPUTER SECURITY BREACH LAW, Mont. Code Ann. §§ 30-14-1704(1), *et seq.*

1281. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Montana Subclass, repeats and alleges Paragraphs 1-1280, as if fully alleged herein. This claim is brought individually under the laws of Montana and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding computer security.

1282. Blackbaud is a business that owns or licenses computerized data that includes "Personal Information" as defined by Mont. Code Ann. § 30-14-1704(4)(b). Blackbaud also maintains computerized data that includes Private Information which Blackbaud does not own. Accordingly, it is subject to Mont. Code Ann. § 30-14-1704(1) and (2).

1283. Plaintiff and Montana Subclass members' Private Information (*e.g.*, SSNs) includes "Personal Information" covered by Mont. Code Ann. § 30-14-1704(4)(b).

1284. Blackbaud is required to give immediate notice of a breach of security of a data system to owners of Private Information which Blackbaud does not own, including Plaintiff and Montana Subclass members, pursuant to Mont. Code Ann. § 30-14-1704(2).

1285. Blackbaud is required to accurately notify Plaintiff and Montana Subclass members if it discovers a security breach or receives notice of a security breach which may have compromised Private Information which Blackbaud owns or licenses, without unreasonable delay under Mont. Code Ann. § 30-14-1704(1).

1286. Because Blackbaud was aware of a security breach, Blackbaud had an obligation to disclose the data breach as mandated by Mont. Code Ann. § 30-14-1704(1) and (2).

1287. Pursuant to Mont. Code Ann. § 30-14-1705, violations of Mont. Code Ann. § 30-14-1704 are unlawful practices under Mont. Code Ann. § 30-14-103, Montana's Consumer Protection Act.

1288. As a direct and proximate result of Blackbaud's violations of Mont. Code Ann. § 30-14-1704(1) and (2), Plaintiff and Montana Subclass members suffered damages and will continue to suffer damages, as described above.

1289. Plaintiff and Montana Subclass members seek relief under Mont. Code Ann. § 30-14-133, including actual damages and injunctive relief.

COUNT 56: MONTANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT, M.C.A. §§ 30-14-101, *et seq.*

1290. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Montana Subclass, repeats and alleges Paragraphs 1-1289, as if fully alleged herein. This claim is brought individually under the laws of Montana and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair trade practices and consumer protection.

1291. Blackbaud is a "person" as defined by MCA § 30-14-102(6).

1292. Plaintiff and Montana Subclass members are “consumers” as defined by MCA § 30-14-102(1).

1293. Blackbaud advertised, offered, or sold goods or services in Montana and engaged in trade or commerce directly or indirectly affecting the people of Montana, as defined by MCA § 30-14-102(8).

1294. Blackbaud engaged in unfair and deceptive acts and practices in the conduct of trade or commerce, in violation MCA § 30-14-103, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Montana Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Montana Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Montana Subclass members’ Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Montana Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Montana Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Montana Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Montana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1295. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1296. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Montana Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Montana Subclass members into believing they did not need to take actions to secure their identities.

1297. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Montana Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Montana Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1298. Blackbaud's acts described above are unfair and offend public policy; they are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

1299. Blackbaud acted intentionally, knowingly, and maliciously to violate Montana's Unfair Trade Practices and Consumer Protection Act, and recklessly disregarded Plaintiff and Montana Subclass members' rights.

1300. As a direct and proximate result of Blackbaud's unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, Plaintiff and Montana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1301. Plaintiff and Montana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of \$500, treble damages, restitution, attorneys' fees and costs, injunctive relief, and other relief that the Court deems appropriate.

CLAIMS ON BEHALF OF THE NEBRASKA SUBCLASS

COUNT 57: NEBRASKA CONSUMER PROTECTION ACT, Neb. Rev. Stat. §§ 59-1601, *et seq.*

1302. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nebraska Subclass, repeats and alleges Paragraphs 1-1301, as if fully alleged herein. This claim is brought individually under the laws of Nebraska and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

1303. Blackbaud and Nebraska Subclass members are each a “person” as defined by Neb. Rev. Stat. § 59-1601(1).

1304. Blackbaud advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska, as defined by Neb. Rev. Stat. § 59-1601.

1305. Blackbaud engaged in unfair and deceptive acts and practices in conducting trade and commerce, in violation of Neb. Rev. Stat. § 59-1602, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Nebraska Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Nebraska Subclass members’ Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Montana Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Nebraska Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1306. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1307. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Nebraska Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Nebraska Subclass members into believing they did not need to take actions to secure their identities.

1308. As a direct and proximate result of Blackbaud's unfair and deceptive acts and practices, Plaintiff and Nebraska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1309. Blackbaud's unfair and deceptive acts and practices complained of herein affected the public interest, including the large percentage of Nebraskans affected by the Data Breach.

1310. Plaintiff and Nebraska Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, the greater of either (1) actual damages or (2) \$1,000, civil penalties, and reasonable attorneys' fees and costs.

**COUNT 58: NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT,
Neb. Rev. Stat. §§ 87-301, *et seq.***

1311. The Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Nebraska Subclass, repeats and alleges Paragraphs 1-1310, as if fully alleged herein. This claim is brought individually under the laws of Nebraska and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

1312. Blackbaud and Nebraska Subclass members are “persons” as defined by Neb. Rev. Stat. § 87-301(19).

1313. Blackbaud advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska.

1314. Blackbaud engaged in deceptive trade practices in the course of its business, in violation of Neb. Rev. Stat. §§ 87-302(a)(5), (8), and (10), including:

- a. Represented that goods and services have characteristics, uses, benefits, or qualities that they do not have;
- b. Represented that goods and services are of a particular standard, quality, or grade if they are of another; and
- c. Advertised its goods and services with intent not to sell them as advertised and in a manner calculated or tending to mislead or deceive.
- d. Blackbaud’s deceptive trade practices include:
- e. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Nebraska Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- f. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- g. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;

- h. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Nebraska Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- i. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- j. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Nebraska Subclass members of the Data Breach;
- k. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- l. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Nebraska Subclass members' Private Information; and
- m. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1315. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1316. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Nebraska Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Nebraska Subclass members into believing they did not need to take actions to secure their identities.

1317. Blackbaud intended to mislead Plaintiff and Nebraska Subclass members and induce them to rely on its misrepresentations and omissions.

1318. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in

business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Nebraska Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Nebraska Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1319. Blackbaud acted intentionally, knowingly, and maliciously to violate Nebraska's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nebraska Subclass members' rights.

1320. As a direct and proximate result of Blackbaud's deceptive trade practices, Plaintiff and Nebraska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1321. Blackbaud's deceptive trade practices complained of herein affected consumers at large, including the large percentage of Nebraskans affected by the Data Breach.

1322. Plaintiff and Nebraska Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEVADA SUBCLASS

COUNT 59: NEVADA DECEPTIVE TRADE PRACTICES ACT, Nev. Rev. Stat. Ann. §§ 598.0903, *et seq.*

1323. The Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Nevada Subclass, repeats and alleges Paragraphs 1-1322, as if fully alleged herein. This claim is brought individually under the laws of Nevada and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

1324. Blackbaud advertised, offered, or sold goods or services in Nevada and engaged in trade or commerce directly or indirectly affecting the people of Nevada.

1325. Blackbaud engaged in deceptive trade practices in the course of its business or occupation, in violation of Nev. Rev. Stat. §§ 598.0915 and 598.0923, including:

- a. Knowingly making a false representation as to the characteristics, uses, and benefits of goods or services for sale in violation of Nev. Rev. Stat. § 598.0915(5);
- b. Representing that goods or services for sale are of a particular standard, quality, or grade when Blackbaud knew or should have known that they are of another standard, quality, or grade in violation of Nev. Rev. Stat. § 598.0915(7);
- c. Advertising goods or services with intent not to sell them as advertised in violation of Nev. Rev. Stat. § 598.0915(9);
- d. Failing to disclose a material fact in connection with the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(2); and
- e. Violating state and federal statutes or regulations relating to the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(3).

1326. Blackbaud’s deceptive trade practices in the course of its business or occupation include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Nevada Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nevada Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Nevada's data security statute, Nev. Rev. Stat. § 603A.210, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Nevada Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nevada Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Nevada's data security statute, Nev. Rev. Stat. § 603A.210;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Nevada Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Nevada Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Nevada's data security statute, Nev. Rev. Stat. § 603A.210.

1327. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1328. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Nevada Subclass members, that their

Private Information was not exposed and misled Plaintiffs and the Nevada Subclass members into believing they did not need to take actions to secure their identities.

1329. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Nevada Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Nevada Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1330. Blackbaud acted intentionally, knowingly, and maliciously to violate Nevada's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nevada Subclass members' rights.

1331. As a direct and proximate result of Blackbaud's deceptive trade practices, Plaintiff and Nevada Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1332. Plaintiff and Nevada Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW HAMPSHIRE SUBCLASS

COUNT 60: NOTICE OF SECURITY BREACH, N.H. Rev. Stat. Ann. §§ 359-C:20(I)(A), *et seq.*

1333. The Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the New Hampshire Subclass, repeats and alleges Paragraphs 1-1332, as if fully alleged herein. This claim is brought individually under the laws of New Hampshire and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding notice of a security breach.

1334. Blackbaud is a business that owns or licenses computerized data that includes “personal information” as defined by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

1335. Plaintiff and New Hampshire Subclass members’ Private Information includes “personal Information” as covered under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

1336. Blackbaud is required to accurately notify Plaintiff and New Hampshire Subclass members if Blackbaud becomes aware of a breach of its data security program in which misuse of Private Information has occurred or is reasonably likely to occur, as soon as possible under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

1337. Because Blackbaud was aware of a security breach in which misuse of Private Information has occurred or is reasonably likely to occur, Blackbaud had an obligation to disclose the data breach in a timely and accurate fashion as mandated by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

1338. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

1339. As a direct and proximate result of Blackbaud's violations of N.H. Rev. Stat. Ann. § 359-C:20(I)(a), Plaintiff and New Hampshire Subclass members suffered damages and will continue to suffer damages, as described above.

1340. Plaintiff and New Hampshire Subclass members seek relief under N.H. Rev. Stat. Ann. § 359-C:21(I), including actual damages and injunctive relief.

**COUNT 61: NEW HAMPSHIRE CONSUMER PROTECTION ACT,
N.H.R.S.A. §§ 358-A, *et seq.***

1341. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Hampshire Subclass, repeats and alleges Paragraphs 1-1340, as if fully alleged herein. This claim is brought individually under the laws of New Hampshire and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

1342. Blackbaud is a "person" under the New Hampshire Consumer Protection.

1343. Blackbaud advertised, offered, or sold goods or services in New Hampshire and engaged in trade or commerce directly or indirectly affecting the people of New Hampshire, as defined by N.H.R.S.A. § 358-A:1.

1344. Blackbaud engaged in unfair and deceptive acts or practices in the ordinary conduct of its trade or business, in violation of N.H.R.S.A. § 358-A:2, including:

- a. Representing that its goods or services have characteristics, uses, or benefits that they do not have in violation of N.H.R.S.A. § 358-A:2.V;
- b. Representing that its goods or services are of a particular standard or quality if they are of another in violation of N.H.R.S.A. § 358-A:2.VII; and
- c. Advertising its goods or services with intent not to sell them as advertised in violation of N.H.R.S.A. § 358-A:2.IX.
- d. Blackbaud's unfair and deceptive acts and practices include:
- e. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New Hampshire Subclass members'

- Private Information, which was a direct and proximate cause of the Data Breach;
- f. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
 - g. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Hampshire Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
 - h. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and New Hampshire Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
 - i. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Hampshire Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
 - j. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and New Hampshire Subclass members of the Data Breach;
 - k. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
 - l. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New Hampshire Subclass members' Private Information; and
 - m. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Hampshire Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1345. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1346. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the New Hampshire Subclass members,

that their Private Information was not exposed and misled Plaintiffs and the New Hampshire Subclass members into believing they did not need to take actions to secure their identities.

1347. Blackbaud acted intentionally, knowingly, and maliciously to violate New Hampshire's Consumer Protection Act, and recklessly disregarded Plaintiff and New Hampshire Subclass members' rights. Blackbaud's acts and practices went beyond the realm of strictly private transactions.

1348. As a direct and proximate result of Blackbaud's unfair and deceptive acts and practices, Plaintiff and New Hampshire Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1349. Plaintiff and New Hampshire Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, equitable relief (including injunctive relief), restitution, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS

COUNT 62: NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT, N.J. Stat. Ann. §§ 56:8-163, *et seq.*

1350. The New Jersey Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeats and alleges Paragraphs 1-1349, as if fully alleged herein. This claim is brought individually under the laws of New Jersey and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer security.

1351. Blackbaud is a business that compiles or maintains computerized records that include “personal information” on behalf of another business under N.J. Stat. Ann. § 56:8-163(b).

1352. Plaintiff and New Jersey Subclass members’ Private Information includes “personal information” covered under N.J. Stat. Ann. §§ 56:8-163, *et seq.*

1353. Under N.J. Stat. Ann. § 56:8-163(b), “[a]ny business . . . that compiles or maintains computerized records that include Personal Information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers . . . of any breach of security of the computerized records immediately following discovery, if the Personal Information was, or is reasonably believed to have been, accessed by an unauthorized person.”

1354. Because Blackbaud discovered a breach of its security system in which Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, Blackbaud had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, *et seq.*

1355. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated N.J. Stat. Ann. § 56:8-163(b).

1356. As a direct and proximate result of Blackbaud’s violations of N.J. Stat. Ann. § 56:8-163(b), Plaintiff and New Jersey Subclass members suffered the damages, and will continue to suffer damages, as described above.

1357. Plaintiff and New Jersey Subclass members seek relief under N.J. Stat. Ann. § 56:8-19, including treble damages, attorneys’ fees and costs, and injunctive relief.

CLAIMS ON BEHALF OF THE NEW MEXICO SUBCLASS

COUNT 63: NEW MEXICO UNFAIR PRACTICES ACT, N.M. Stat. Ann. §§ 57-12-2, *et seq.*

1358. The Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the New Mexico Subclass, repeats and alleges Paragraphs 1-1357, as if fully alleged herein. This claim is brought individually under the laws of New Mexico and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair practices.

1359. Blackbaud is a “person” as meant by N.M. Stat. Ann. § 57-12-2.

1360. Blackbaud was engaged in “trade” and “commerce” as meant by N.M. Stat. Ann. § 57-12-2(C) when engaging in the conduct alleged.

1361. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2, *et seq.*, prohibits both unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce.

1362. Blackbaud engaged in unconscionable, unfair, and deceptive acts and practices in connection with the sale of goods or services in the regular course of its trade or commerce, including the following:

- a. Knowingly representing that its goods and services have characteristics, benefits, or qualities that they do not have, in violation of N.M. Stat. Ann. § 57-12-2(D)(5);
- b. Knowingly representing that its goods and services are of a particular standard or quality when they are of another in violation of N.M. Stat. Ann. § 57-12-2(D)(7);
- c. Knowingly using exaggeration, innuendo, or ambiguity as to a material fact or failing to state a material fact where doing so deceives or tends to deceive in violation of N.M. Stat. Ann. § 57-12-2(D)(14);
- d. Taking advantage of the lack of knowledge, experience, or capacity of its consumers to a grossly unfair degree to Plaintiff and the New Mexico Subclass’ detriment in violation of N.M. Stat. Ann. § 57-2-12(E)(1); and

- e. Performing these acts and practices in a way that results in a gross disparity between the value received by Plaintiff and the New Mexico Subclass and the price paid, to their detriment, in violation of N.M. Stat. § 57-2-12(E)(2).
- f. Blackbaud's unfair, deceptive, and unconscionable acts and practices include:
- g. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New Mexico Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- h. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- i. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Mexico Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4, which was a direct and proximate cause of the Data Breach;
- j. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and New Mexico Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- k. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Mexico Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4;
- l. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and New Mexico Subclass members of the Data Breach;
- m. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- n. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New Mexico Subclass members' Private Information; and
- o. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security

and privacy of Plaintiff and New Mexico Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4.

1363. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1364. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the New Mexico Subclass members, that their Private Information was not exposed and misled Plaintiffs and the New Mexico Subclass members into believing they did not need to take actions to secure their identities.

1365. Blackbaud intended to mislead Plaintiff and New Mexico Subclass members and induce them to rely on its misrepresentations and omissions.

1366. Blackbaud acted intentionally, knowingly, and maliciously to violate New Mexico's Unfair Practices Act, and recklessly disregarded Plaintiff and New Mexico Subclass members' rights.

1367. As a direct and proximate result of Blackbaud's unfair, deceptive, and unconscionable trade practices, Plaintiff and New Mexico Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1368. Plaintiff and New Mexico Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages or statutory damages of \$100

(whichever is greater), treble damages or statutory damages of \$300 (whichever is greater), and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT 64: NEW YORK GENERAL BUSINESS LAW, N.Y. Gen. Bus. Law §§ 349, *et seq.*

1369. The New York Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, repeats and alleges Paragraphs 1-1368, as if fully alleged herein. This claim is brought individually under the laws of New York and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive acts or practices.

1370. Blackbaud engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New York Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and New York Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Private Information, including duties imposed by the

- FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and New York Subclass members of the Data Breach;
 - g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
 - h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New York Subclass members' Private Information; and
 - i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1371. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1372. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the New York Subclass members, that their Private Information was not exposed and misled Plaintiffs and the New York Subclass members into believing they did not need to take actions to secure their identities.

1373. Blackbaud acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass members' rights.

1374. As a direct and proximate result of Blackbaud's deceptive and unlawful acts and practices, Plaintiff and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial

accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1375. Blackbaud's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the millions of New Yorkers affected by the Data Breach.

1376. The above deceptive and unlawful practices and acts by Blackbaud caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

1377. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

CLAIMS ON BEHALF OF THE NORTH CAROLINA SUBCLASS

COUNT 65: NORTH CAROLINA IDENTITY THEFT PROTECTION ACT, N.C. Gen. Stat. §§ 75-60, *et seq.*

1378. The North Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and alleges Paragraphs 1-1377, as if fully alleged herein. This claim is brought individually under the laws of North Carolina and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding identity theft.

1379. Blackbaud is a business that owns or licenses computerized data that includes "Personal Information" within the meaning of N.C. Gen. Stat. § 75-61(1) and N.C. Gen. Stat. § 75-65..

1380. Plaintiff and North Carolina Subclass members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

1381. Blackbaud is required to accurately notify Plaintiff and North Carolina Subclass members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

1382. Plaintiff and North Carolina Subclass members' Private Information includes "Personal Information" as covered under N.C. Gen. Stat. § 75-61(10).

1383. Because Blackbaud discovered a security breach and had notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), Blackbaud had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

1384. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated N.C. Gen. Stat. § 75-65.

1385. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. § 75-1.1.

1386. As a direct and proximate result of Blackbaud's violations of N.C. Gen. Stat. § 75-65, Plaintiff and North Carolina Subclass members suffered damages, and will continue to suffer damages, as described above.

1387. Plaintiff and North Carolina Subclass members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorney's fees.

**COUNT 66: NORTH CAROLINA UNFAIR TRADE PRACTICES ACT,
N.C. Gen. Stat. Ann. §§ 75-1.1, *et seq.***

1388. The North Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and alleges Paragraphs 1-1387, as if fully alleged herein. This claim is brought individually under the laws of North

Carolina and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair trade practices.

1389. Blackbaud advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

1390. Blackbaud engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and North Carolina Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and North Carolina Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and North Carolina Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and North Carolina Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.
- j. Failing to properly notify Plaintiff and North Carolina Subclass of the Data Breach violation of the North Carolina Identity Theft Protection Act, N.C. Gen. Stat. § 75-65.

1391. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1392. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the North Carolina Subclass members, that their Private Information was not exposed and misled Plaintiffs and the North Carolina Subclass members into believing they did not need to take actions to secure their identities.

1393. Blackbaud intended to mislead Plaintiff and North Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

1394. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the North Carolina Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the North

Carolina Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1395. Blackbaud acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and North Carolina Subclass members' rights.

1396. As a direct and proximate result of Blackbaud's unfair and deceptive acts and practices, Plaintiff and North Carolina Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1397. Blackbaud's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

1398. Plaintiff and North Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NORTH DAKOTA SUBCLASS

COUNT 67: NOTICE OF SECURITY BREACH FOR PERSONAL INFORMATION, N.D. Cent. Code §§ 51-30-02, *et seq.*

1399. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Dakota Subclass, repeats and alleges Paragraphs 1-1398, as if fully alleged herein. This claim is brought individually under the laws of North Dakota and on behalf of all other natural persons whose Private Information was compromised as a result of

the Data Breach and reside in states having similar laws regarding the security of personal information.

1400. Blackbaud is a business that owns or licenses computerized data that includes “Personal Information” as defined by N.D. Cent. Code § 51-30-01(4). Blackbaud also maintains computerized data that includes Private Information which Blackbaud does not own. Accordingly, it is subject to N.D. Cent. Code §§ 51-30-02 and 03.

1401. Plaintiff and North Dakota Subclass members’ Private Information (*e.g.*, SSNs) includes “Personal Information” covered by N.D. Cent. Code § 51-30-01(4).

1402. Blackbaud is required to give immediate notice of a breach of security of a data system to owners of Private Information which Blackbaud does not own, including Plaintiff and North Dakota Subclass members, pursuant to N.D. Cent. Code § 51-30-03.

1403. Blackbaud is required to accurately notify Plaintiff and North Dakota Subclass members if it discovers a security breach or receives notice of a security breach which may have compromised Private Information which Blackbaud owns or licenses, in the most expedient time possible and without unreasonable delay under N.D. Cent. Code § 51-30-02.

1404. Because Blackbaud was aware of a security breach, Blackbaud had an obligation to disclose the data breach as mandated by N.D. Cent. Code §§ 51-30-02 and 51-30-03.

1405. Pursuant to N.D. Cent. Code § 51-30-07, violations of N.D. Cent. Code §§ 51-30-02 and 51-30-03 are unlawful sales or advertising practices which violate chapter 51-15 of the North Dakota Century Code.

1406. As a direct and proximate result of Blackbaud’s violations of N.D. Cent. Code §§ 51-30-02 and 51-30-03, Plaintiff and North Dakota Subclass members suffered damages, and will continue to suffer damages, as described above.

1407. Plaintiff and North Dakota Subclass members seek relief under N.D. Cent. Code §§ 51-15-01 *et seq.*, including actual damages and injunctive relief.

**COUNT 68: NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT,
N.D. Cent. Code §§ 51-15-01, *et seq.***

1408. The Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the North Dakota Subclass, repeats and alleges Paragraphs 1-1407, as if fully alleged herein. This claim is brought individually under the laws of North Dakota and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unlawful sales or advertising.

1409. Blackbaud, Plaintiff, and each member of the North Dakota Subclass is a “person,” as defined by N.D. Cent. Code § 51-15-01(4).

1410. Blackbaud sells and advertises “merchandise,” as defined by N.D. Cent. Code § 51-15-01(3) and (5).

1411. Blackbaud advertised, offered, or sold goods or services in North Dakota and engaged in trade or commerce directly or indirectly affecting the people of North Dakota.

1412. Blackbaud engaged in deceptive, false, fraudulent, misrepresentative, unconscionable, and substantially injurious acts and practices in connection with the sale and advertisement of merchandise, in violation of N.D. Cent. Code § 51-15-01, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and North Dakota Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Dakota Subclass members’ Private Information, including duties imposed by the FTC Act,

- 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and North Dakota Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
 - e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Dakota Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
 - f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and North Dakota Subclass members of the Data Breach;
 - g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
 - h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and North Dakota Subclass members' Private Information; and
 - i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Dakota Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1413. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1414. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the North Dakota Subclass members, that their Private Information was not exposed and misled Plaintiffs and the North Dakota Subclass members into believing they did not need to take actions to secure their identities.

1415. The Blackbaud's above-described acts and practices caused substantial injury to Plaintiff and North Dakota Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

1416. Blackbaud intended to mislead Plaintiff and North Dakota Subclass members and induce them to rely on its misrepresentations and omissions.

1417. Blackbaud acted intentionally, knowingly, and maliciously to violate North Dakota's Unlawful Sales or Advertising Law, and recklessly disregarded Plaintiff and North Dakota Subclass members' rights.

1418. As a direct and proximate result of Blackbaud's deceptive, unconscionable, and substantially injurious practices, Plaintiff and North Dakota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1419. Plaintiff and North Dakota Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, restitution, treble damages, civil penalties, and attorneys' fees, costs, and disbursements.

CLAIMS ON BEHALF OF THE OHIO SUBCLASS

COUNT 69: OHIO DECEPTIVE TRADE PRACTICES ACT, Ohio Rev. Code §§ 4165.01, *et seq.*

1420. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeats and alleges Paragraphs 1-1419, as if fully alleged herein. This claim is brought individually under the laws of Ohio and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

1421. Blackbaud, Plaintiff, and Ohio Subclass members are a "person," as defined by Ohio Rev. Code § 4165.01(D).

1422. Blackbaud advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

1423. Blackbaud engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including:

- a. Representing that its goods and services have characteristics, uses, benefits, or qualities that they do not have, in violation of Ohio Rev. Code § 4165.02(A)(7);
- b. Representing that its goods and services are of a particular standard or quality when they are of another, in violation of Ohio Rev. Code § 4165.02(A)(9); and
- c. Advertising its goods and services with intent not to sell them as advertise, in violation of Ohio Rev. Code § 4165.02(A)(11).
- d. Blackbaud's deceptive trade practices include:
- e. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Ohio Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- f. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- g. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- h. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Ohio Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- i. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- j. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Ohio Subclass members of the Data Breach;
- k. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

1. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Ohio Subclass members' Private Information; and
- m. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1424. Blackbaud did not engage in reasonable data security measures and/or did not follow its own data security measures in place at the time of the Data Breach.

1425. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1426. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Ohio Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Ohio Subclass members into believing they did not need to take actions to secure their identities.

1427. Blackbaud intended to mislead Plaintiff and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

1428. Blackbaud acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass members' rights.

1429. As a direct and proximate result of Blackbaud's deceptive trade practices, Plaintiff and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1430. Plaintiff and Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE OKLAHOMA SUBCLASS

COUNT 70: OKLAHOMA CONSUMER PROTECTION ACT, Okla. Stat. tit. 15, §§ 751, *et seq.*

1431. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oklahoma Subclass, repeats and alleges Paragraphs 1-1430, as if fully alleged herein. This claim is brought individually under the laws of Oklahoma and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

1432. Blackbaud is a "person," as meant by Okla. Stat. tit. 15, § 752(1).

1433. Blackbaud's advertisements, offers of sales, sales, and distribution of goods, services, and other things of value constituted "consumer transactions" as meant by Okla. Stat. tit. 15, § 752(2).

1434. Blackbaud, in the course of its business, engaged in unlawful practices in violation of Okla. Stat. tit. 15, § 753, including the following:

- a. Making false representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of its consumer transactions, in violation of Okla. Stat. tit. 15, § 753(5);
- b. Representing, knowingly or with reason to know, that the subjects of its consumer transactions were of a particular standard when they were of another, in violation of Okla. Stat. tit 15, § 753(7);
- c. Advertising, knowingly or with reason to know, the subjects of its consumer transactions with intent not to sell as advertised, in violation of Okla. Stat. tit 15, § 753 (8);
- d. Committing unfair trade practices that offend established public policy and was immoral, unethical, oppressive, unscrupulous, and substantially

injurious to consumers as defined by section 752(14), in violation of Okla. Stat. tit. 15, § 753(20); and

- e. Committing deceptive trade practices that deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person as defined by section 752(13), in violation of Okla. Stat. tit. 15, § 753(20).

1435. Blackbaud's unlawful practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Oklahoma Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oklahoma Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Oklahoma Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oklahoma Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Oklahoma Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Oklahoma Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oklahoma Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1436. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1437. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Oklahoma Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Oklahoma Subclass members into believing they did not need to take actions to secure their identities.

1438. Blackbaud intended to mislead Plaintiff and Oklahoma Subclass members and induce them to rely on its misrepresentations and omissions.

1439. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Oklahoma Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Oklahoma Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1440. The above unlawful practices and acts by Blackbaud were immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial injury to Plaintiff and Oklahoma Subclass members.

1441. Blackbaud acted intentionally, knowingly, and maliciously to violate Oklahoma's Consumer Protection Act, and recklessly disregarded Plaintiff and Oklahoma Subclass members' rights.

1442. As a direct and proximate result of Blackbaud's unlawful practices, Plaintiff and Oklahoma Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1443. Plaintiff and Oklahoma Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE OREGON SUBCLASS

COUNT 71: OREGON UNLAWFUL TRADE PRACTICES ACT, Or. Rev. Stat. §§ 646.608, *et seq.*

1444. The Oregon Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oregon Subclass, repeats and alleges Paragraphs 1-1443, as if fully alleged herein. This claim is brought individually under the laws of Oregon and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unlawful trade practices.

1445. Blackbaud is a "person," as defined by Or. Rev. Stat. § 646.605(4).

1446. Blackbaud engaged in the sale of "goods and services," as defined by Or. Rev. Stat. § 646.605(6)(a).

1447. Blackbaud sold "goods or services," as defined by Or. Rev. Stat. § 646.605(6)(a).

1448. Blackbaud advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

1449. Blackbaud engaged in unlawful practices in the course of its business and occupation, in violation of Or. Rev. Stat. § 646.608, included the following:

- a. Representing that its goods and services have approval, characteristics, uses, benefits, and qualities that they do not have, in violation of Or. Rev. Stat. § 646.608(1)(e);
- b. Representing that its goods and services are of a particular standard or quality if they are of another, in violation of Or. Rev. Stat. § 646.608(1)(g);
- c. Advertising its goods or services with intent not to provide them as advertised, in violation of Or. Rev. Stat. § 646.608(1)(i); and
- d. Concurrent with tender or delivery of its goods and services, failing to disclose any known material defect, in violation of Or. Rev. Stat. § 646.608(1)(t).
- e. Blackbaud's unlawful practices include:
- f. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Oregon Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- g. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- h. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*, which was a direct and proximate cause of the Data Breach;
- i. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Oregon Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- j. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*;
- k. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Oregon Subclass members of the Data Breach;

1. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- m. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Oregon Subclass members' Private Information; and
- n. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*

1450. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1451. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Oregon Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Oregon Subclass members into believing they did not need to take actions to secure their identities.

1452. Blackbaud intended to mislead Plaintiff and Oregon Subclass members and induce them to rely on its misrepresentations and omissions.

1453. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Oregon Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Oregon

Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1454. Blackbaud acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Plaintiff and Oregon Subclass members' rights.

1455. As a direct and proximate result of Blackbaud's unlawful practices, Plaintiff and Oregon Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1456. Plaintiff and Oregon Subclass members seek all monetary and non-monetary relief allowed by law, including equitable relief, actual damages or statutory damages of \$200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE PUERTO RICO SUBCLASS

COUNT 72: CITIZEN INFORMATION ON DATA BANKS SECURITY ACT, P.R. Laws Ann. tit. 10, §§ 4051, *et seq.*

1457. Plaintiffs, on behalf of the Puerto Rico Subclass, repeat and allege Paragraphs 1-1456, as if fully alleged herein. This claim is brought individually under the laws of Puerto Rico and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding information on data banks security.

1458. Blackbaud is the owner and custodian of databases that include "Personal information" as defined by P.R. Laws Ann. tit. 10, § 4051(a), and is therefore subject to P.R. Laws Ann. tit. 10, § 4052.

1459. Plaintiff and Puerto Rico Subclass members' Private Information includes "Personal information" as covered under P.R. Laws Ann. tit. 10, § 4051(a).

1460. Blackbaud is required to accurately notify Plaintiff and Puerto Rico Subclass members following discovery or notification of a breach of its data security program as expeditiously as possible under P.R. Laws Ann. tit. 10, § 4052.

1461. Because Blackbaud discovered a breach of its data security program, Blackbaud had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by P.R. Laws Ann. tit. 10, § 4052.

1462. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated P.R. Laws Ann. tit. 10, § 4052.

1463. As a direct and proximate result of Blackbaud's violations of P.R. Laws Ann. tit. 10, § 4052, Plaintiff and Puerto Rico Subclass members suffered damages, and will continue to suffer damages, as described above.

1464. Plaintiff and Puerto Rico Subclass members seek relief under P.R. Laws Ann. tit. 10, § 4055, including actual damages and injunctive relief.

CLAIMS ON BEHALF OF THE RHODE ISLAND SUBCLASS

COUNT 73: RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT, R.I. Gen. Laws §§ 6-13.1, *et seq.*

1465. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Rhode Island Subclass, repeats and alleges Paragraphs 1-1464, as if fully alleged herein. This claim is brought individually under the laws of Rhode Island and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

1466. Plaintiff and Rhode Island Subclass members are each a “person,” as defined by R.I. Gen. Laws § 6-13.1-1(3).

1467. Plaintiff and Rhode Island Subclass members purchased goods and services for personal, family, or household purposes.

1468. Blackbaud advertised, offered, or sold goods or services in Rhode Island and engaged in trade or commerce directly or indirectly affecting the people of Rhode Island, as defined by R.I. Gen. Laws § 6-13.1-1(5).

1469. Blackbaud engaged in unfair and deceptive acts and practices, in violation of R.I. Gen. Laws § 6-13.1-2, including:

- a. Representing that its goods and services have characteristics, uses, and benefits that they do not have (R.I. Gen. Laws § 6-13.1-52(6)(v));
- b. Representing that its goods and services are of a particular standard or quality when they are of another (R.I. Gen. Laws § 6-13.1-52(6)(vii));
- c. Advertising goods or services with intent not to sell them as advertised (R.I. Gen. Laws § 6-13.1-52(6)(ix));
- d. Engaging in any other conduct that similarly creates a likelihood of confusion or misunderstanding (R.I. Gen. Laws § 6-13.1-52(6)(xii));
- e. Engaging in any act or practice that is unfair or deceptive to the consumer (R.I. Gen. Laws § 6-13.1-52(6)(xiii)); and
- f. Using other methods, acts, and practices that mislead or deceive members of the public in a material respect (R.I. Gen. Laws § 6-13.1-52(6)(xiv)).

1470. Blackbaud’s unfair and deceptive acts include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Rhode Island Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Rhode Island Subclass members’

- Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Rhode Island Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
 - e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Rhode Island Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2;
 - f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Rhode Island Subclass members of the Data Breach;
 - g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
 - h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Rhode Island Subclass members' Private Information; and
 - i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Rhode Island Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2.

1471. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1472. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Rhode Island Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Rhode Island Subclass members into believing they did not need to take actions to secure their identities.

1473. Blackbaud intended to mislead Plaintiff and Rhode Island Subclass members and induce them to rely on its misrepresentations and omissions.

1474. Blackbaud acted intentionally, knowingly, and maliciously to violate Rhode Island's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Rhode Island Subclass members' rights.

1475. As a direct and proximate result of Blackbaud's unfair and deceptive acts, Plaintiff and Rhode Island Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1476. Plaintiff and Rhode Island Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$200 per Subclass Member (whichever is greater), punitive damages, injunctive relief, other equitable relief, and attorneys' fees and costs.

COUNT 74: RHODE ISLAND CONFIDENTIALITY OF HEALTH CARE INFORMATION ACT, R.I. Gen. Laws § 5-37.3-1, *et seq.*

1477. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Rhode Island PHI Subclass, repeats and alleges Paragraphs 1-1476, as if fully alleged herein. This claim is brought individually under the laws of Rhode Island and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding the confidentiality of health care information.

1478. The Rhode Island Confidentiality of Health Care Information Act (“CHCIA”) prohibits, among other things, unauthorized disclosure of personally identifiable confidential healthcare information. R.I. Gen. Laws § 5-37.3-1, *et seq.*

1479. Plaintiff provided her PHI to a Social Good Entity which is a “health care provider” as defined by R.I. Gen. Laws § 5-37.3-3(4).

1480. Blackbaud is an “agent” of the Social Good Entity to which Plaintiff provided her PHI and therefore is a “health care provider” as defined by R.I. Gen. Laws § 5-37.3-3(4).

1481. Plaintiff is a “patient”, as defined by R.I. Gen. Laws § 5-37.3-3(12), of the Social Good Entity to which Plaintiff provided her PHI.

1482. Blackbaud stored on its computer system “personally identifiable confidential healthcare information” as defined by R.I. Gen. Laws § 5-37.3-3(13) pertaining to the Plaintiff and the Rhode Island PHI Subclass.

1483. Blackbaud disclosed personally identifiable confidential healthcare information pertaining to the Plaintiff and the Rhode Island PHI Subclass without their written consent and for no other reason permitted by R.I. Gen. Laws § 5-37.3-4.

1484. The affirmative actions of Blackbaud in maintaining the security of its computer system at levels that allowed hackers to improperly access and copy private medical records of the Plaintiff and the Rhode Island PHI Subclass.

1485. Blackbaud failed to establish the security procedures in relation to confidential health care information as required by R.I. Gen. Laws § 5-37.3-4, and therefore violated R.I. Gen. Laws § 5-37.3-4.

1486. The Plaintiff and the Rhode Island PHI Subclass members were injured by Blackbaud’s release or transfer of their confidential health care information and/or failure to

establish security procedures to protect their confidential healthcare information in violation of R.I. Gen. Laws § 5-37.3-4.

1487. Plaintiff and the Rhode Island PHI Subclass seeks relief for Blackbaud's violation of R.I. Gen. Laws § 5-37.3-4, including but not limited to actual damages, punitive damages, declaratory relief, injunctive relief, and/or attorneys' fees and costs, as well as statutory damages of \$5,000 for each knowing and intentional violation.

CLAIMS ON BEHALF OF THE SOUTH DAKOTA SUBCLASS

COUNT 75: SOUTH DAKOTA DECEPTIVE TRADE PRACTICES AND CONSUMER PROTECTION ACT, S.D. Codified Laws §§ 37-24-1, *et seq.*

1488. The South Dakota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the South Dakota Subclass, repeats and alleges Paragraphs 1-1487, as if fully alleged herein. This claim is brought individually under the laws of South Dakota and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices and consumer protection.

1489. Blackbaud is a "person," as defined by S.D. Codified Laws § 37-24-1(8).

1490. Blackbaud advertises and sells "merchandise," as defined by S.D. Codified Laws § 37-24-1(6), (7), & (13).

1491. Blackbaud advertised, offered, or sold goods or services in South Dakota and engaged in trade or commerce directly or indirectly affecting the people of South Dakota, as defined by S.D. Codified Laws § 37-24-1(6), (7), & (13).

1492. Blackbaud knowingly engaged in deceptive acts or practices, misrepresentation, concealment, suppression, or omission of material facts in connection with the sale and advertisement of goods or services, in violation of S.D. Codified Laws § 37-24-6, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and South Dakota Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Dakota Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and South Dakota Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Dakota Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and South Dakota Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and South Dakota Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Dakota Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1493. Blackbaud intended to mislead Plaintiff and South Dakota Subclass members and induce them to rely on its misrepresentations and omissions.

1494. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the South Dakota Subclass members,

that their Private Information was not exposed and misled Plaintiffs and the South Dakota Subclass members into believing they did not need to take actions to secure their identities.

1495. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1496. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the South Dakota Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the South Dakota Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1497. Blackbaud had a duty to disclose the above facts because members of the public, including Plaintiff and the South Dakota Subclass, reposed a trust and confidence in Blackbaud. Indeed, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the South Dakota Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the South Dakota Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth

of which they could not have discovered. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the South Dakota Subclass, and Blackbaud because consumers are unable to fully protect their interests with regard to their data, and have placed trust and confidence in Blackbaud. Blackbaud's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the South Dakota Subclass that contradicted these representations.

1498. As a direct and proximate result of Blackbaud's deceptive acts or practices, misrepresentations, and concealment, suppression, and/or omission of material facts, Plaintiff and South Dakota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1499. Blackbaud's violations present a continuing risk to Plaintiff and South Dakota Subclass members as well as to the general public.

1500. Plaintiff and South Dakota Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE TENNESSEE SUBCLASS

COUNT 76: TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT, Tenn. Code Ann. §§ 47-18-2107, *et seq.*

1501. The Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeats and alleges Paragraphs 1-1500, as if fully alleged herein. This claim is brought individually under the laws of Tennessee and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding personal consumer information.

1502. This claim is brought individually under the laws of Tennessee and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding personal consumer information.

1503. Blackbaud is a business that owns or licenses computerized data that includes Personal Information as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

1504. Plaintiff and Tennessee Subclass members’ Private Information include “Personal Information” as covered under Tenn. Code Ann. § 47-18-2107(a)(3)(A).

1505. Blackbaud is required to accurately notify Plaintiff and Tennessee Subclass members following discovery or notification of a breach of its data security program in which unencrypted Private Information was, or is reasonably believed to have been, acquired by an unauthorized person, in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

1506. Because Blackbaud discovered a breach of its security system in which unencrypted Private Information was, or is reasonably believed to have been, acquired by an unauthorized person, Blackbaud had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

1507. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated Tenn. Code Ann. § 47-18-2107(b).

1508. As a direct and proximate result of Blackbaud's violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Subclass members suffered damages, and will continue to suffer damages, as described above.

1509. Plaintiff and Tennessee Subclass members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages, injunctive relief, and treble damages.

CLAIMS ON BEHALF OF THE TEXAS SUBCLASS

COUNT 77: DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT, Texas Bus. & Com. Code §§ 17.41, *et seq.*

1510. The Texas Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Texas Subclass, repeats and alleges Paragraphs 1-1509, as if fully alleged herein. This claim is brought individually under the laws of Texas and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

1511. Blackbaud is a “person,” as defined by Tex. Bus. & Com. Code § 17.45(3).

1512. Plaintiffs and the Texas Subclass members are “consumers,” as defined by Tex. Bus. & Com. Code § 17.45(4).

1513. Blackbaud advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

1514. Blackbaud engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;
- b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and
- c. Advertising goods or services with intent not to sell them as advertised.
- d. Blackbaud's false, misleading, and deceptive acts and practices include:
- e. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Texas Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- f. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- g. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;
- h. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Texas Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- i. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;
- j. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Texas Subclass members of the Data Breach;
- k. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- l. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Texas Subclass members' Private Information; and
- m. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45,

HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

1515. Blackbaud intended to mislead Plaintiff and Texas Subclass members and induce them to rely on its misrepresentations and omissions.

1516. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1517. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Texas Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Texas Subclass members into believing they did not need to take actions to secure their identities.

1518. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Texas Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Texas Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1519. Blackbaud had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted professional standards in its industry. This duty arose because members of the public,

including Plaintiffs and the Texas Subclass, repose a trust and confidence in Blackbaud. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and the Texas Subclass, and Blackbaud because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Blackbaud. Blackbaud's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the Texas Subclass that contradicted these representations.

1520. Blackbaud engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Blackbaud engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

1521. Consumers, including Plaintiffs and Texas Subclass members, lacked knowledge about deficiencies in Blackbaud's data security because this information was known exclusively by Blackbaud. Consumers also lacked the ability, experience, or capacity to secure the Private Information in Blackbaud's possession or to fully protect their interests with regard to their data. Plaintiffs and Texas Subclass members lack expertise in information security matters and do not have access to Blackbaud's systems in order to evaluate its security controls. Blackbaud took advantage of its special skill and access to Private Information to hide its inability to protect the security and confidentiality of Plaintiffs and Texas Subclass members' Private Information.

1522. Blackbaud intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that

would result. The unfairness resulting from Blackbaud's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from Blackbaud's unconscionable business acts and practices, exposed Plaintiffs and Texas Subclass members to a wholly unwarranted risk to the safety of their Private Information and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and Texas Subclass members cannot mitigate this unfairness because they cannot undo the data breach.

1523. Blackbaud acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff and Texas Subclass members' rights.

1524. As a direct and proximate result of Blackbaud's unconscionable and deceptive acts or practices, Plaintiffs and Texas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information. Blackbaud's unconscionable and deceptive acts or practices were a producing cause of Plaintiffs' and Texas Subclass members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

1525. Blackbaud's violations present a continuing risk to Plaintiffs and Texas Subclass members as well as to the general public.

1526. Plaintiffs and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for

each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

COUNT 78: TEXAS HEALTH & SAFETY CODE § 241.152

1527. The Texas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Texas PHI Subclass, repeats and alleges Paragraphs 1-1526, as if fully alleged herein. This claim is brought individually under the laws of Texas and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding health and safety.

1528. Plaintiff brings this cause of action in the District Court of South Carolina as the Judicial Panel on Multidistrict Litigation created this MDL, and this Court is handling all pretrial matters related to the Data Breach and causes of action alleged concerning same.

1529. Texas law provides that, except under circumstances that do not apply here, a hospital or an agent or employee of a hospital may not disclose health care information about a patient to any person other than the patient or the patient's legally authorized representative without the written authorization of the patient or the patient's legally authorized representative.

See Tex. Health & Safety Code § 241.152.

1530. At all relevant times, the Social Good Entity to which Plaintiff provided his PHI was a "hospital" within the meaning of Tex. Health & Safety Code § 241.152.

1531. At all relevant times, Blackbaud stored "health care information" of the Plaintiff and other members of the Texas PHI Subclass as construed under Tex. Health & Safety Code § 241.153.

1532. Plaintiff and the other Texas PHI Subclass members did not provide Blackbaud consent to release their health care records to third parties.

1533. Blackbaud had a duty to adopt and implement reasonable safeguards for the security of all health care information it maintains pursuant to Tex. Health & Safety Code § 241.155.

1534. Blackbaud negligently or intentionally disclosed and released Plaintiff and the Texas PHI Subclass members' health care information inasmuch as it did not implement adequate security protocols to prevent unauthorized access to health care information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data breach or otherwise comply with HIPAA data security requirements.

1535. As a direct and proximate result of Blackbaud's negligent or intentional acts, it disclosed and released Plaintiff's health care information to third parties without the Plaintiff's consent and caused injury to the Plaintiff and the Texas PHI Subclass.

1536. Accordingly, Plaintiff, individually and on behalf of members of the Texas PHI Subclass, seeks compensatory damages, injunctive relief plus costs and attorney fees. *See* Tex. Health & Safety Code § 241.156.

CLAIMS ON BEHALF OF THE UTAH SUBCLASS

COUNT 79: UTAH CONSUMER SALES PRACTICES ACT, Utah Code §§ 13-11-1, *et seq.*

1537. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Utah Subclass, repeats and alleges Paragraphs 1-1536, as if fully alleged herein. This claim is brought individually under the laws of Utah and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer sales practices.

1538. Blackbaud is a "person," as defined by Utah Code § 13-11-1(5).

1539. Blackbaud is a “supplier,” as defined by Utah Code § 13-11-1(6), because it regularly solicits, engages in, or enforces “consumer transactions,” as defined by Utah Code § 13-11-1(2).

1540. Blackbaud engaged in deceptive and unconscionable acts and practices in connection with consumer transactions, in violation of Utah Code § 13-11-4 and Utah Code § 13-11-5, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Utah Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Utah Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Utah Protection of Personal Information Act, Utah Code § 13-44-201, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Utah Subclass members’ Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Utah Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Utah Protection of Personal Information Act, Utah Code § 13-44-201;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Utah Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Utah Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Subclass members’ Private Information; and

- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the Utah Protection of Personal Information Act, Utah Code § 13-44-201.

1541. Blackbaud intended to mislead Plaintiff and Utah Subclass members and induce them to rely on its misrepresentations and omissions.

1542. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1543. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Utah Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Utah Subclass members into believing they did not need to take actions to secure their identities.

1544. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Utah Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Utah Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1545. Blackbaud had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted professional standards in its industry. This duty arose because members of the public, including Plaintiff and the Utah Subclass, reposed a trust and confidence in Blackbaud. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Utah Subclass, and Blackbaud because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Blackbaud. Blackbaud's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Utah Subclass that contradicted these representations.

1546. Blackbaud intentionally or knowingly engaged in deceptive acts or practices, violating Utah Code § 13-11-4(2) by:

- a. Indicating that the subject of a consumer transaction has sponsorship, approval, performance characteristics, accessories, uses, or benefits, if it has not;
- b. Indicating that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not;
- c. Indicating that the subject of a consumer transaction has been supplied in accordance with a previous representation, if it has not;
- d. Indicating that the subject of a consumer transaction will be supplied in greater quantity (*e.g.* more data security) than the supplier intends.

1547. Blackbaud engaged in unconscionable acts and practices that were oppressive and led to unfair surprise, as shown in the setting, purpose, and effect of those acts and practices. Blackbaud's acts and practices unjustly imposed hardship on Plaintiff and the Utah Subclass by imposing on them, through no fault of their own, an increased and imminent risk of fraud and

identity theft; substantial cost in time and expenses related to monitoring their financial accounts for fraudulent activity; and lost value of their Private Information. The deficiencies in Blackbaud's data security, and the material misrepresentations and omissions concerning those deficiencies, led to unfair surprise to Plaintiff and the Utah Subclass when the Data Breach occurred.

1548. In addition, there was an overall imbalance in the obligations and rights imposed by the consumer transactions in question, based on the mores and industry standards of the time and place where they occurred. There is a substantial imbalance between the obligations and rights of consumers, such as Plaintiff and the Utah Subclass, and Blackbaud, which has control over the Private Information in its possession. Industry standards—including those reflected in the security requirements of the GLBA—also dictate that Blackbaud adequately secure the Private Information in its possession.

1549. Blackbaud's acts and practices were also procedurally unconscionable because consumers, including Plaintiff and the Utah Subclass, had no practicable option but to have their Private Information stored in Blackbaud's systems if they wanted to participate in the nation's financial system. Blackbaud exploited this imbalance in power, and the asymmetry of information about its data security, to profit by inadequately securing the Private Information in its systems.

1550. As a direct and proximate result of Blackbaud's unconscionable and deceptive acts or practices, Plaintiffs and Utah Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1551. Blackbaud's violations present a continuing risk to Plaintiffs and Utah Subclass members as well as to the general public.

1552. Plaintiff and Utah Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, statutory damages of \$2,000 per violation under Utah Code §§ 13-11-19, *et seq.*; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE VERMONT SUBCLASS

COUNT 80: VERMONT CONSUMER FRAUD ACT, Vt. Stat. Ann. tit. 9, §§ 2451, *et seq.*

1553. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Vermont Subclass, repeats and alleges Paragraphs 1-1552, as if fully alleged herein. This claim is brought individually under the laws of Vermont and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud.

1554. Plaintiff and Vermont Subclass members are "consumers," as defined by Vt. Stat. Ann. tit. 9, § 2451a(a).

1555. Blackbaud's conduct as alleged herein related to "goods" or "services" for personal, family, or household purposes, as defined by Vt. Stat. Ann. tit. 9, § 2451a(b).

1556. Blackbaud is a "seller," as defined by Vt. Stat. Ann. tit. 9, § 2451a(c).

1557. Blackbaud advertised, offered, or sold goods or services in Vermont and engaged in trade or commerce directly or indirectly affecting the people of Vermont.

1558. Blackbaud engaged in unfair and deceptive acts or practices, in violation of Vt. Stat. tit. 9, § 2453(a), including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Vermont Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Vermont Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Vermont Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Vermont Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Vermont Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Vermont Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Vermont Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1559. Blackbaud intended to mislead Plaintiff and Vermont Subclass members and induce them to rely on its misrepresentations and omissions.

1560. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1561. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Vermont Subclass members, that

their Private Information was not exposed and misled Plaintiffs and the Vermont Subclass members into believing they did not need to take actions to secure their identities.

1562. Under the circumstances, consumers had a reasonable interpretation of Blackbaud's representations and omissions.

1563. Blackbaud had a duty to disclose these facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted professional standards in its industry. This duty arose because members of the public, including Plaintiff and the Vermont Subclass, reposed a trust and confidence in Blackbaud. Indeed, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Vermont Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Vermont Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Vermont Subclass, and Blackbaud because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Blackbaud. Blackbaud's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Vermont Subclass that contradicted these representations.

1564. Blackbaud's acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1565. The injury to consumers was and is substantial because it was non-trivial and non-speculative; and involved a concrete monetary injury and/or an unwarranted risk to the safety of their Private Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1566. Consumers could not have reasonably avoided injury because Blackbaud's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Blackbaud created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1567. Blackbaud's inadequate data security had no countervailing benefit to consumers or to competition.

1568. Blackbaud is presumed, as a matter of law under Vt. Stat. Ann. tit. 9, § 2457, to have intentionally violated the Vermont Consumer Protection Act because it failed to sell goods or services in the manner and of the nature advertised or offered.

1569. Blackbaud acted intentionally, knowingly, and maliciously to violate Vermont's Consumer Fraud Act, and recklessly disregarded Plaintiff and Vermont Subclass members' rights.

1570. As a direct and proximate result of Blackbaud's unfair and deceptive acts or practices, Plaintiffs and Vermont Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages,

including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1571. Blackbaud's violations present a continuing risk to Plaintiffs and Vermont Subclass members as well as to the general public.

1572. Plaintiff and Vermont Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, restitution, actual damages, disgorgement of profits, treble damages, punitive/exemplary damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE VIRGIN ISLANDS SUBCLASS

COUNT 81: IDENTITY THEFT PREVENTION ACT, V.I. Code tit. 14 §§ 2208, *et seq.*

1573. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and allege Paragraphs 1-1572, as if fully alleged herein. This claim is brought individually under the laws of Virgin Islands and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding identity theft.

1574. Blackbaud is a business that owns or licenses computerized data that includes Personal Information as defined by V.I Code tit. 14 § 2201(a). Blackbaud also maintains computerized data that includes "Personal identifying information" which Blackbaud does not own. Accordingly, it is subject to V.I Code tit. 14 §§ 2208(a) and (b).

1575. Virgin Islands Subclass members' Private Information (*e.g.*, SSNs) includes "Personal identifying information" covered by V.I Code tit. 14 § 2201(a).

1576. Blackbaud is required to give immediate notice of a breach of security of a data system to owners of Private Information which Blackbaud does not own, including Virgin Islands Subclass members, pursuant to V.I Code tit. 14 § 2208(b).

1577. Blackbaud is required to accurately notify Virgin Islands Subclass members if it discovers a security breach, or receives notice of a security breach which may have compromised Private Information which Blackbaud owns or licenses, in the most expedient time possible and without unreasonable delay under V.I Code tit. 14 § 2208(a).

1578. Because Blackbaud was aware of a security breach, Blackbaud had an obligation to disclose the data breach as mandated by V.I Code tit. 14 § 2208.

1579. As a direct and proximate result of Blackbaud's violations of V.I Code tit. 14 §§ 2208(a) and (b), Virgin Islands Subclass members suffered damages, and will continue to suffer damages, as described above.

1580. Virgin Islands Subclass members seek relief under V.I Code tit. 14 §§ 2211(a) and (b), including actual damages, and injunctive relief.

COUNT 82: VIRGIN ISLANDS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, V.I. Code tit. 12A, §§ 301, *et seq.*

1581. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and allege Paragraphs 1-1580, as if fully alleged herein. This claim is brought individually under the laws of the Virgin Islands and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer fraud and deceptive business practices.

1582. Blackbaud is a “person,” as defined by V.I. Code tit. 12A, § 303(h).

1583. Plaintiff and Virgin Islands Subclass members are “consumers,” as defined by V.I. Code tit. 12A, § 303(d).

1584. Blackbaud advertised, offered, or sold goods or services in the Virgin Islands and engaged in trade or commerce directly or indirectly affecting the people of the Virgin Islands.

1585. Blackbaud engaged in unfair and deceptive acts and practices, in violation of V.I. Code tit. 12A, § 304, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Virgin Islands Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Virgin Islands Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Virgin Islands Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Virgin Islands Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1586. Blackbaud's acts and practices were "unfair" under V.I. Code tit. 12A, § 304 because they caused or were likely to cause substantial injury to consumers which was not

reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1587. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Virgin Islands Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Virgin Islands Subclass members into believing they did not need to take actions to secure their identities.

1588. The injury to consumers from Blackbaud's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and/or an unwarranted risk to the safety of their Private Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1589. Consumers could not have reasonably avoided injury because Blackbaud's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Blackbaud created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1590. Blackbaud's inadequate data security had no countervailing benefit to consumers or to competition.

1591. Blackbaud's acts and practices were "deceptive" under V.I. Code tit. 12A, §§ 303 & 304 because Blackbaud made representations or omissions of material facts that had the capacity, tendency or effect of deceiving or misleading consumers, including Plaintiff and Virgin Islands Subclass members.

1592. Blackbaud intended to mislead Plaintiff and Virgin Island Subclass members and induce them to rely on its misrepresentations and omissions.

1593. Blackbaud's representations and omissions were material because they were likely to unfairly influence or deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1594. Blackbaud had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted professional standards in its industry. This duty arose because members of the public, including Plaintiff and the Virgin Islands Subclass, reposed a trust and confidence in Blackbaud. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Virgin Islands Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Virgin Islands Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Virgin Islands Subclass—and Blackbaud, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Blackbaud. Blackbaud's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while

purposefully withholding material facts from Plaintiff and the Virgin Islands Subclass that contradicted these representations.

1595. Blackbaud acted intentionally, knowingly, and maliciously to violate the Virgin Island's Consumer Fraud and Deceptive Business Practices Act, and recklessly disregarded Plaintiff and Virgin Islands Subclass members' rights. Blackbaud intentionally hid the inadequacies in its data security, callously disregarding the rights of consumers.

1596. As a direct and proximate result of Blackbaud's unfair and deceptive acts or practices, Plaintiff and Virgin Islands Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1597. Blackbaud's violations present a continuing risk to Plaintiff and Virgin Islands Subclass members as well as to the general public.

1598. Plaintiff and Virgin Islands Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory, consequential, treble, punitive, and equitable damages under V.I. Code tit. 12A, § 331; injunctive relief; and reasonable attorneys' fees and costs.

**COUNT 83: VIRGIN ISLANDS CONSUMER PROTECTION LAW,
V.I. Code tit. 12A, §§101, *et seq.***

1599. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and allege Paragraphs 1-1598, as if fully alleged herein. This claim is brought individually under the laws of the Virgin Islands and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

1600. Blackbaud is a "merchant," as defined by V.I. Code tit. 12A, § 102(e).

1601. Plaintiff and Virgin Islands Subclass members are “consumers,” as defined by V.I. Code tit. 12A, § 102(d).

1602. Blackbaud sells and offers for sale “consumer goods” and “consumer services,” as defined by V.I. Code tit. 12A, § 102(c).

1603. Blackbaud engaged in deceptive acts and practices, in violation of V.I. Code tit. 12A, § 101, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Virgin Islands Subclass members’ Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Virgin Islands Subclass members’ Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Virgin Island Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Virgin Islands Subclass members’ Private Information; and

- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1604. Blackbaud's acts and practices were "deceptive trade practices" under V.I. Code tit. 12A, § 102(a) because Blackbaud:

- a. Represented that goods or services have sponsorship, approval, accessories, characteristics, ingredients, uses, benefits, or quantities that they do not have; or that goods or services are of particular standard, quality, grade, style or model, if they are of another;
- b. Used exaggeration, innuendo or ambiguity as to a material fact or failure to state a material fact if such use deceives or tends to deceive;
- c. Offered goods or services with intent not to sell them as offered; and
- d. Stated that a consumer transaction involves consumer rights, remedies or obligations that it does not involve.

1605. Blackbaud's acts and practices were also "deceptive" under V.I. Code tit. 12A, § 101 because Blackbaud made representations or omissions of material facts that had the capacity, tendency or effect of deceiving or misleading consumers, including Plaintiff and Virgin Islands Subclass members.

1606. Blackbaud intended to mislead Plaintiff and Virgin Islands Subclass members and induce them to rely on its misrepresentations and omissions.

1607. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1608. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Virgin Island Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Virgin Island Subclass members into believing they did not need to take actions to secure their identities.

1609. Blackbaud had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted professional standards in its industry. This duty arose because members of the public, including Plaintiff and the Virgin Islands Subclass, repose a trust and confidence in Blackbaud.

1610. Indeed, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Virgin Islands Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public.

1611. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Virgin Islands Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Virgin Islands Subclass—and Blackbaud, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Blackbaud. Blackbaud's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virgin Islands Subclass that contradicted these representations.

1612. Blackbaud acted intentionally, knowingly, and maliciously to violate the Virgin Island's Consumer Protection Law, and recklessly disregarded Plaintiff and Virgin Island Subclass members' rights.

1613. As a direct and proximate result of Blackbaud's deceptive acts or practices, Plaintiff and Virgin Islands Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1614. Blackbaud's violations present a continuing risk to Plaintiff and Virgin Islands Subclass members as well as to the general public.

1615. Plaintiff and Virgin Islands Subclass members seek all monetary and non-monetary relief allowed by law, including declaratory relief; injunctive relief; the greater of actual damages or \$500 per violation; compensatory, consequential, treble, and punitive damages; disgorgement; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE WASHINGTON SUBCLASS

COUNT 84: WASHINGTON DATA BREACH NOTICE ACT, Wash. Rev. Code §§ 19.255.010, *et seq.*

1616. The Washington Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and alleges Paragraphs 1-1615, as if fully alleged herein. This claim is brought individually under the laws of Washington and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding data breach notice.

1617. Blackbaud is a business that owns or licenses computerized data that includes "personal information" as defined by Wash. Rev. Code § 19.255.010(1).

1618. Plaintiff and Washington Subclass members' Private Information includes "personal information" as covered under Wash. Rev. Code § 19.255.010(5).

1619. Blackbaud is required to accurately notify Plaintiff and Washington Subclass members following discovery or notification of the breach of its data security program if Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, in the most expedient time possible and without unreasonable delay under Wash. Rev. Code § 19.255.010(1).

1620. Because Blackbaud discovered a breach of its security system in which Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, Blackbaud had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code § 19.255.010(1).

1621. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated Wash. Rev. Code § 19.255.010(1).

1622. As a direct and proximate result of Blackbaud’s violations of Wash. Rev. Code § 19.255.010(1), Plaintiff and Washington Subclass members suffered damages, and will continue to suffer damages, as described above.

1623. Plaintiff and Washington Subclass members seek relief under Wash. Rev. Code §§ 19.255.040, including actual damages and injunctive relief.

**COUNT 85: WASHINGTON CONSUMER PROTECTION ACT,
Wash. Rev. Code Ann. §§ 19.86.020, *et seq.***

1624. The Washington Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and alleges Paragraphs 1-1623, as if fully alleged herein. This claim is brought individually under the laws of Washington and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

1625. Blackbaud is a “person,” as defined by Wash. Rev. Code Ann. § 19.86.010(1).

1626. Blackbaud advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

1627. Blackbaud engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Washington Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Washington Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Washington Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Washington Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1628. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1629. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Washington Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Washington Subclass members into believing they did not need to take actions to secure their identities.

1630. Blackbaud acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and Washington Subclass members' rights.

1631. Blackbaud's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, including, but not limited to Wash. Rev. Code §§ 19.255.010, *et seq.*. Alternatively, Blackbaud's conduct is injurious to the public interest because it has injured Plaintiff and Washington Subclass members, had the capacity to injure persons, and has the capacity to injure other persons, and has the capacity to injure persons. Further, its conduct affected the public interest, including the millions of Washingtonians affected by the Data Breach.

1632. As a direct and proximate result of Blackbaud's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Washington Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1633. Plaintiff and Washington Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE WEST VIRGINIA SUBCLASS

COUNT 86: WEST VIRGINIA CONSUMER CREDIT AND PROTECTION ACT, W. Va. Code §§ 46A-6-101, *et seq.*

1634. The Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the West Virginia Subclass, repeats and alleges Paragraphs 1-1633, as if fully alleged herein. This claim is brought individually under the laws of West Virginia and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer credit and protection.

1635. Plaintiff and West Virginia Subclass members are "consumers," as defined by W. Va. Code § 46A-6-102(2).

1636. Blackbaud engaged in "consumer transactions," as defined by W. Va. Code § 46A-6-102(2).

1637. Blackbaud advertised, offered, or sold goods or services in West Virginia and engaged in trade or commerce directly or indirectly affecting the people of West Virginia, as defined by W. Va. Code § 46A-6-102(6).

1638. Plaintiff sent a demand for relief on behalf of the West Virginia Subclass pursuant to W. Va. Code § 46A-6-106(c) on February 24, 2021. Blackbaud has not cured its unfair and deceptive acts and practices.

1639. Blackbaud engaged in unfair and deceptive business acts and practices in the conduct of trade or commerce, in violation of W. Va. Code § 46A-6-104, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and West Virginia Subclass members'

- Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
 - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and West Virginia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
 - d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and West Virginia Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
 - e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and West Virginia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
 - f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and West Virginia Subclass members of the Data Breach;
 - g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
 - h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and West Virginia Subclass members' Private Information; and
 - i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and West Virginia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1640. Blackbaud's unfair and deceptive acts and practices also violated W. Va. Code § 46A-6-102(7), including:

- a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;
- b. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model if they are of another;

- c. Advertising goods or services with intent not to sell them as advertised;
- d. Engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding;
- e. Using deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of goods or services, whether or not any person has in fact been misled, deceived or damaged thereby; and
- f. Advertising, displaying, publishing, distributing, or causing to be advertised, displayed, published, or distributed in any manner, statements and representations with regard to the sale of goods or the extension of consumer credit, which are false, misleading or deceptive or which omit to state material information which is necessary to make the statements therein not false, misleading or deceptive.

1641. Blackbaud's unfair and deceptive acts and practices were unreasonable when weighed against the need to develop or preserve business, and were injurious to the public interest, under W. Va. Code § 46A-6-101.

1642. Blackbaud's acts and practices were additionally "unfair" under W. Va. Code § 46A-6-104 because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1643. The injury to consumers from Blackbaud's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and/or an unwarranted risk to the safety of their Private Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1644. Consumers could not have reasonably avoided injury because Blackbaud's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers

about the inadequacy of its data security, Blackbaud created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

1645. Blackbaud's inadequate data security had no countervailing benefit to consumers or to competition.

1646. Blackbaud's acts and practices were additionally "deceptive" under W. Va. Code § 46A-6-104 because Blackbaud made representations or omissions of material facts that misled or were likely to mislead reasonable consumers, including Plaintiff and West Virginia Subclass members.

1647. Blackbaud intended to mislead Plaintiff and West Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

1648. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1649. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the West Virginia Subclass members, that their Private Information was not exposed and misled Plaintiffs and the West Virginia Subclass members into believing they did not need to take actions to secure their identities.

1650. Had Blackbaud disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the West Virginia Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate

state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the West Virginia Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1651. Blackbaud had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted professional standards in its industry. This duty arose because members of the public, including Plaintiff and the West Virginia Subclass, reposed a trust and confidence in Blackbaud. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the West Virginia Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the West Virginia Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the West Virginia Subclass—and Blackbaud, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Blackbaud. Blackbaud's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;
- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the West Virginia Subclass that contradicted these representations.

1652. Blackbaud's omissions were legally presumed to be equivalent to active misrepresentations because Blackbaud intentionally prevented Plaintiff and West Virginia Subclass members from discovering the truth regarding Blackbaud's inadequate data security.

1653. Blackbaud acted intentionally, knowingly, and maliciously to violate West Virginia's Consumer Credit and Protection Act, and recklessly disregarded Plaintiff and West Virginia Subclass members' rights. Blackbaud's unfair and deceptive acts and practices were likely to cause serious harm.

1654. As a direct and proximate result of Blackbaud's unfair and deceptive acts or practices and Plaintiff and West Virginia Subclass members' purchase of goods or services, Plaintiff and West Virginia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1655. Blackbaud's violations present a continuing risk to Plaintiff and West Virginia Subclass members as well as to the general public.

1656. Plaintiff and West Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or \$200 per violation under W. Va. Code § 46A-6-106(a); restitution, injunctive and other equitable relief; punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE WISCONSIN SUBCLASS

COUNT 87: WISCONSIN DECEPTIVE TRADE PRACTICES ACT, Wis. Stat. § 100.18

1657. The Plaintiff(s) identified above (“Plaintiff,” for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeats and alleges Paragraphs 1-1656, as if fully alleged herein. This claim is brought individually under the laws of Wisconsin and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding deceptive trade practices.

1658. Blackbaud is a “person, firm, corporation or association,” as defined by Wis. Stat. § 100.18(1).

1659. Plaintiff and Wisconsin Subclass members are members of “the public,” as defined by Wis. Stat. § 100.18(1).

1660. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Blackbaud to members of the public for sale, use, or distribution, Blackbaud made, published, circulated, placed before the public or caused (directly or indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of Wis. Stat. § 100.18(1).

1661. Blackbaud also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of Wis. Stat. § 100.18(9).

1662. Blackbaud’s deceptive acts, practices, plans, and schemes include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Wisconsin Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wisconsin Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Wisconsin Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wisconsin Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Wisconsin Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Wisconsin Subclass members' Private Information;
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wisconsin Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505; and
- j. Violating the Wisconsin Notice of Unauthorized Acquisition of Personal Information Act, Wis. Stat. §§ 134.98(2), *et seq.*, by failing to timely and accurately notify victims of the Data Breach.

1663. Blackbaud intended to mislead Plaintiff and Wisconsin Subclass members and induce them to rely on its misrepresentations and omissions.

1664. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Blackbaud's data security and ability to protect the confidentiality of consumers' Private Information.

1665. Blackbaud's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Wisconsin Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Wisconsin Subclass members into believing they did not need to take actions to secure their identities.

1666. Blackbaud had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted professional standards in its industry. This duty arose because members of the public, including Plaintiff and the Wisconsin Subclass, reposed a trust and confidence in Blackbaud. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Wisconsin Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Wisconsin Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Wisconsin Subclass—and Blackbaud, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Blackbaud. Blackbaud's duty to disclose also arose from its:

- a. Possession of exclusive knowledge regarding the security of the data in its systems;

- b. Active concealment of the state of its security; and/or
- c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Wisconsin Subclass that contradicted these representations.

1667. Blackbaud's failure to disclose the above-described facts is the same as actively representing that those facts do not exist.

1668. Blackbaud acted intentionally, knowingly, and maliciously to violate the Wisconsin Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Wisconsin Subclass members' rights.

1669. As a direct and proximate result of Blackbaud's deceptive acts or practices, Plaintiff and Wisconsin Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1670. Blackbaud had an ongoing duty to all Blackbaud customers to refrain from deceptive acts, practices, plans, and schemes under Wis. Stat. § 100.18.

1671. Plaintiff and Wisconsin Subclass members seek all monetary and non-monetary relief allowed by law, including damages, reasonable attorneys' fees, and costs under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

**COUNT 88: WISCONSIN CONFIDENTIALITY OF HEALTH RECORDS LAW,
Wis. St. § 146.82, § 142.84**

1672. The Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeats and alleges Paragraphs 1-1671, as if fully alleged herein. This claim is brought individually under the laws of Wisconsin and on behalf of all other

natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding the confidentiality of health records.

1673. The Wisconsin Confidentiality of Health Records Law prohibits, among other things, unauthorized disclosure of patient healthcare records. Wis. Stat. §146.82.

1674. Plaintiff provided her PHI to a Social Good Entity which is a “health care provider” as defined by Wis. Stat. § 146.81(1).

1675. Plaintiff is a “patient”, as defined by Wis. Stat. § 146.81(3), of the Social Good Entity to which Plaintiff provided her PHI.

1676. Blackbaud is a “covered entity” for purposes of Wis. Stat. §146.82 and had a duty not to re-disclose any healthcare records in its possession regarding the Plaintiff and members of the Wisconsin Subclass. Wis. Stat. §146.82.

1677. Blackbaud re-disclosed healthcare records pertaining to the Plaintiff and members of the Wisconsin PHI Subclass without their consent and for no other reason permitted by either Wis. Stat. §146.82(5) or §610.70, and therefore violated Wis. Stat. §146.82.

1678. The affirmative actions of Blackbaud in maintaining the security of its computer system at levels that allowed hackers to improperly access and copy private healthcare records of the Plaintiff and the Wisconsin PHI Subclass. Blackbaud actively and affirmatively allowed the hackers to see and obtain the healthcare records of the Plaintiff and members of the Wisconsin PHI Subclass.

1679. Plaintiff and the Wisconsin PHI Subclass members were injured and have suffered damages from Blackbaud’s illegal disclosure and negligent release of their healthcare records in violation of Wis. Stat. §146.82.

1680. Plaintiff individual and on behalf of the Wisconsin PHI Subclass seeks relief under Wis. Stat. § 146.84 including but not limited to actual damages, nominal damages, exemplary damages of up to \$25,000 for knowing and willful violations and up to \$1,000 for negligent violations, statutory penalties, injunctive relief, and/or attorneys' fees and costs.

CLAIMS ON BEHALF OF THE WYOMING SUBCLASS

COUNT 89: COMPUTER SECURITY BREACH; NOTICE TO AFFECTED PERSONS, Wyo. Stat. Ann. §§ 40-12-502(a), *et seq.*

1681. The Wyoming Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wyoming Subclass, repeats and alleges Paragraphs 1-1680, as if fully alleged herein. This claim is brought individually under the laws of Wyoming and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding computer security.

1682. Blackbaud is a business that owns or licenses computerized data that includes Private Information as defined by Wyo. Stat. Ann. § 40-12-502(a).

1683. Plaintiff and Wyoming Subclass members' Private Information includes "personal identifying information" as covered under Wyo. Stat. Ann. § 40-12-502(a).

1684. Blackbaud is required to accurately notify Plaintiff and Wyoming Subclass members when it becomes aware of a breach of its data security program if the misuse of personal identifying information has occurred or is reasonably likely to occur, in the most expedient time possible and without unreasonable delay under Wyo. Stat. Ann. § 40-12-502(a).

1685. Because Blackbaud was aware of a breach of its data security program in which the misuse of personal identifying information has occurred or is reasonably likely to occur, Blackbaud had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Wyo. Stat. Ann. § 40-12-502(a).

1686. By failing to disclose the Data Breach in a timely and accurate manner, Blackbaud violated Wyo. Stat. Ann. § 40-12-502(a).

1687. As a direct and proximate result of Blackbaud's violations of Wyo. Stat. Ann. § 40-12-502(a), Plaintiff and Wyoming Subclass members suffered damages, and will continue to suffer damages, as described above.

1688. Plaintiff and Blackbaud Subclass members seek relief under Wyo. Stat. Ann. § 40-12-502(f), including actual damages and equitable relief.

**COUNT 90: VIOLATION OF THE WYOMING CONSUMER PROTECTION ACT,
Wyo. Stat. Ann. § 40-12-101, *et seq.***

1689. The Wyoming Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wyoming Subclass, repeats and alleges Paragraphs 1-1688, as if fully alleged herein. This claim is brought individually under the laws of Wyoming and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

1690. Blackbaud is a "person, firm, corporation or association," as defined by Wyo. Stat. Ann. § 40-12-102(a)(i), and conducts "consumer transactions" within the meaning of Wyo. Stat. Ann. § 40-12-102(a)(ii).

1691. Plaintiff and Wyoming Subclass members are "persons" within the meaning of Wyo. Stat. Ann. § 40-12-102(a)(i).

1692. Blackbaud engaged in unlawful deceptive trade practices in the course of its business, in violation of Wyo. Stat. Ann. § 40-12-105, including:

- a. Knowingly making a false representation as to the characteristics of its products and services;
- b. Representing that its services are of a particular standard, quality or grad, though Blackbaud knew or should have known that they were otherwise; and

- c. Representing that its services are available to the consumers for a reason that does not exist.

1693. Blackbaud's deceptive acts, practices, plans, and schemes include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Wyoming Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wyoming Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Wisconsin Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wyoming Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505;
- f. Failing to timely and adequately notify the Social Good Entities, Plaintiffs, and Wyoming Subclass members of the Data Breach;
- g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;
- h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Wyoming Subclass members' Private Information; and
- i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wyoming Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

1694. Had Blackbaud disclosed to Plaintiff and the Wyoming Subclass members that its data systems were not secure and, thus, vulnerable to attack, Blackbaud would have been unable

to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Blackbaud was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and the Wyoming Subclass. Blackbaud accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Blackbaud held itself out as maintaining a secure platform for Private Information data, Plaintiff and the Wyoming Subclass members acted reasonably in relying on Blackbaud's misrepresentations and omissions, the truth of which they could not have discovered.

1695. Blackbaud acted intentionally, knowingly, and maliciously to violate Wyoming's Consumer Protection Act, and recklessly disregarded Plaintiff and the Wyoming Subclass members' rights.

1696. As a direct and proximate result of Blackbaud's unfair or deceptive trade practices, Plaintiff and the Wyoming Subclass members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their Private Information.

1697. Plaintiff and the Wyoming Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, and reasonable attorneys' fees and costs pursuant to Wyo. Stat. Ann. § 40-12

IX. PRAAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

- A. For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class and Subclasses;
- B. For equitable relief enjoining Blackbaud from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class

and Subclass members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and the Class members or to mitigate further harm;

C. For equitable relief compelling Blackbaud to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief compelling Blackbaud to update and correct statements made to Plaintiffs, Class members, government officials, and the general public about the Data Breach, which have failed to put Plaintiffs and Class members on notice of the significant risks of future, irreparable harm they face as a result of the Data Breach, and to allow Plaintiffs and Class members to take action to mitigate that harm;

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Blackbaud's wrongful conduct;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including reasonable expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

X. JURY TRIAL DEMAND

Plaintiffs hereby demand a jury trial for all claims so triable.

Dated this 21st day of December, 2021 Respectfully submitted,

/s/ Marlon E. Kimpson

Marlon E. Kimpson (SC Bar No. 17042)*
MOTLEY RICE LLC
28 Bridgeside Boulevard
Mount Pleasant, SC 29464
Tel.: (843) 216-9000
Fax: (843) 216-9027
Email: mkimpson@motleyrice.com

Amy E. Keller*
DICELLO LEVITT GUTZLER LLC
Ten North Dearborn Street, Sixth Floor
Chicago, IL 60602
Tel: (312) 214-7900
Fax: (312) 253-1443
Email: akeller@dicellosevitt.com

Krysta Kauble Pachman*
SUSMAN GODFREY LLP
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Tel: (310) 789-3100
Fax: (310) 789-3150
Email: kpachman@susmangodfrey.com

Harper Segui*
Federal ID No. 10841
**MILBERG COLEMAN BRYSON PHILLIPS
GROSSMAN PLLC**
825 Lowcountry Blvd.,
Suite 101
Mount Pleasant, SC 29464
Tel: (919) 600-5000
Fax: (919) 600-5035
Email: hsegui@milberg.com

**Plaintiffs' Co-Lead Counsel*

Gretchen Freeman Cappio**
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Tel.: (206) 623-1900
Fax: (206) 623-3384
Email: gcappio@kellerrohrback.com

***Chair of Plaintiffs' Steering Committee*

Desiree Cummings
ROBBINS GELLER RUDMAN & DOWD LLP
420 Lexington Avenue, Suite 1832
New York, NY 10170
Tel: (212) 693-1058
Email: dcummings@rgrdlaw.com

Melissa Emert
**KANTROWITZ, GOLDHAMMER &
GRAIFMAN, PC**
747 Chestnut Ridge Road
Chestnut Ridge, NY 10977
Tel: (866) 574-4682
Fax: (845) 356-4335
Email: memert@kgglaw.com

Kelly Iverson
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
Email: kelly@lcllp.com

Howard Longman
LONGMAN LAW, P.C.
354 Eisenhower Parkway, Suite 1800
Livingston, NJ 07039
Tel: (973) 994-2315
Fax: (973) 994-2319
Email: hlongman@longman.law

Douglas McNamara
**COHEN MILSTEIN SELLERS
& TOLL PLLC**
1100 New York Avenue NW
East Tower, 5th Floor
Washington, DC 20005
Tel: (202) 408-4600
Fax: (202) 408-4699
Email: dmcnamara@cohenmilstein.com

Melissa Weiner
PEARSON, SIMON & WARSHAW, LLP

800 LaSalle Avenue, Suite 2150
Minneapolis, MN 55402
Tel: (612) 389-0600
Fax: (612) 389-0610
Email: mweiner@psqlaw.com

Plaintiffs' Steering Committee

Frank Ulmer
MCCULLEY MCCLUER LLC
701 East Bay Street, Suite 411
Charleston, SC 29403
Tel: (843) 444-5404
Fax: (843) 444-5408
Email: fulmer@mcculleymccluer.com

Plaintiffs' Liaison Counsel